

**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 WILLOUGHBY  
3 HIF088.160

4 ``CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND  
5 PUBLIC-SECTOR RESPONSES  
6 WEDNESDAY, MARCH 28, 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 10:05 a.m.,  
12 in 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, Bono Mack, Bass, Blackburn, Latta, Guthrie,  
16 Kinzinger, Eshoo, Matsui, Barrow, Dingell and Waxman (ex  
17 officio).

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

19 Baum, Senior Policy Advisor/Director of Coalitions; Nicholas  
20 Degani, FCC Detailee; Andy Duberstein, Deputy Press  
21 Secretary; Neil Fried, Chief Counsel, Communications and  
22 Technology; Debbie Keller, Press Secretary; Katie Novaria,  
23 Legislative Clerk; and David Redl, Counsel, Telecom.

|  
24           Mr. {Walden.} Good morning. The Subcommittee on  
25 Communications and the Internet will come to order. The  
26 title of today's hearing is ``Cybersecurity: Threats to  
27 Communications Networks and Public-Sector Responses.''

28           Heeding the call of the House Republican Cybersecurity  
29 Task Force appointed by the Speaker, this subcommittee has  
30 embarked on a series of hearings, as most of you are aware,  
31 to get a complete picture of the cybersecurity challenges  
32 that face our Nation. Today is the third of our hearings on  
33 this topic, having already heard from witnesses in our  
34 previous hearings on the concerns of the private-sector  
35 security firms helping to secure communications networks from  
36 cyber threats as well as the network operators that must  
37 protect their networks while providing the broadband services  
38 that have become the fuel of our economy. Those hearings  
39 provided us with a lot of very, very valuable information. We  
40 appreciate the witnesses who testified. This hearing  
41 continues our subcommittee's review of cybersecurity issues  
42 with a focus on the public sector.

43           In order to further investigate the complex issues that  
44 surround any discussion of cybersecurity, I recently asked a  
45 number of my subcommittee colleagues to serve on a bipartisan  
46 working group tasked with gathering additional information.

47 My vice chairman, Mr. Terry, and Ranking Member Eshoo have  
48 graciously served as co-chairs of the working group for the  
49 last few weeks, and I am very appreciative of their work.  
50 The group also included Representatives Doyle, Matsui,  
51 Kinzinger, and Latta. The members of the working group and  
52 their staffs have met with a number of industry stakeholders,  
53 and throughout their discussions a consistent theme has  
54 emerged: the need for the government and the private sector  
55 to work together to address cybersecurity. The findings of  
56 the working group are consistent with the message we have  
57 heard in our hearings on this matter from the private-sector  
58 perspective.

59 Today, we hear from some of the agencies within our  
60 government that are working to meet these threats, both in  
61 terms of what is being done to promote cybersecurity as well  
62 as how we can better secure our Nation's communications  
63 networks. In this hearing, we are privileged to have five  
64 witnesses that represent parts of the government that work to  
65 address the complex cybersecurity issues our country faces  
66 every day. The work being done by these government agencies  
67 to help address cybersecurity is just the tip of the iceberg  
68 of what we can achieve when our private-sector innovation and  
69 public-sector resources are put to a common task. That is why  
70 I am a co-sponsor of H.R. 3523, which is the Cyber

71 Intelligence Sharing and Protection Act. This bipartisan  
72 bill introduced by my Communications and Technology colleague  
73 and Chairman of the House Permanent Select Committee on  
74 Intelligence, Mike Rogers. H.R. 3523 makes commonsense  
75 changes to the way our government and the private sector  
76 share cyber intelligence without compromising either the  
77 commercial broadband providers or the integrity of the  
78 intelligence community.

79         Similarly, the good work being done by industry  
80 stakeholders at the FCC on the Communications Security,  
81 Reliability and Interoperability Council, or CSRIC, to bring  
82 voluntary best practices to bear on the security of  
83 commercial networks is another example of the type of public-  
84 private cooperation that I think will achieve results without  
85 mandates. It looks very similar to the Australian model that  
86 received favorable reviews at one of our previous hearings.  
87 To remain nimble and effective, codes of conduct like these  
88 should remain voluntary and should involve all stakeholders  
89 in the Internet ecosystem, not just the ISPs.

90         In addition to hearing from these agencies on the good  
91 work that they are doing, I also expect to hear how you think  
92 we can improve the cooperation between the federal government  
93 and private industry as they work to combat cyber threats.  
94 Having heard from the private sector, today's public-sector

95 perspective will give the members of the subcommittee a more  
96 complete picture of the cybersecurity landscape.

97 I thank the panelists for your testimony today. I look  
98 forward to a lively discussion of these issues.

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

100 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
101           Mr. {Walden.} With that, I would yield the remainder of  
102 my time to the gentleman from Nebraska, Mr. Terry.

103           Mr. {Terry.} Thank you, Mr. Chairman, and it is  
104 certainly quite a learning curve from both the Speaker's task  
105 force and the task force that Anna and I have been lucky  
106 enough to oversee.

107           But this is a real threat to our economy and to our  
108 country, and we need to really start thinking seriously about  
109 ways of securing our communications networks, and in that  
110 discussion, not only how but who should be part of that  
111 process, and first I want to commend the Communications  
112 Security and Reliability Interoperability Council, or CSRIC,  
113 for its recent report outlining voluntary best practices that  
114 industry has agreed to implement and ISPs engaging in the  
115 Anti-Bot Code of Conduct and Domain Name System best  
116 practices as well as working to develop a framework to  
117 prevent IP route hijacking is a great start to improving our  
118 overall health and safety of our Nation's networks and  
119 limiting access for attacks. I am confident that this  
120 collaboration will continue to improve.

121           I will state for the record that I have some  
122 reservations concerning giving government agencies like  
123 Department of Homeland Security authority for overseeing or

124 implementing the standards. A, I think we need to focus on  
125 flexibility, and secondly, that department hasn't provided me  
126 the level of confidence that I would want to turn over our  
127 cybersecurity to them. All we have to do is walk into our  
128 airports and visualize my lack of confidence in them.

129         So at this point I will yield back, and I am anxious to  
130 hear from the witnesses.

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

132 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
133           Mr. {Walden.} I now recognize the gentlelady from  
134 California, my friend, Ms. Eshoo, for an opening statement.

135           Ms. {Eshoo.} Thank you, Mr. Chairman, and good morning  
136 to all of my colleagues on the subcommittee, and welcome to  
137 our witnesses. Thank you for being willing to be here today  
138 to instruct us even further on this whole issue of  
139 cybersecurity that we have had a very important series of  
140 hearings and they have been very, very helpful. They have  
141 been outstanding hearings, and both sides of the aisle, I  
142 think, have agreed on that.

143           As has been stated, I am part of the Cybersecurity  
144 Working Group with Congressman Terry, and through the process  
145 that we have followed, our collective staff have gathered  
146 information from key stakeholders and have been focusing on  
147 issues such as supply chain integrity, information sharing,  
148 consumer education, and it is obviously our subcommittee's  
149 jurisdiction in these areas. We have learned that Advanced  
150 Persistent Threats, the APTs, pose a significant risk to our  
151 communications infrastructure, and these sophisticated  
152 threats are often either state sponsored or pursued by  
153 criminal enterprises and they have the potential to lead to  
154 significant theft or manipulation of data and other malicious  
155 activities.

156           So we have our hands full, most frankly, about how to go  
157 at this. Fortunately, there are experts like each one of you  
158 that are working hard, really diligently to protect our  
159 country from cyber threats, so we really look forward to  
160 hearing what you can instruct us on this, and I want to  
161 especially welcome Mr. Hutchinson from Sandia National Labs  
162 Adaptive Network Countermeasures--these are real mouthfuls, I  
163 will tell you--the ANC, the DHS efforts concerning domain  
164 name server security extension and the FCC's recent  
165 recommendations from CSRIC. All of these need to be stitched  
166 together. We can't afford to go into an enlightened endeavor  
167 and end up with silos all over again. I am very sensitive  
168 about that, having been a veteran of the House Intelligence  
169 Committee.

170           So I think to deter cyber criminals, we need to have a  
171 really well-coordinated, comprehensive effort that is going  
172 to promote R&D, consumer education, supply chain integrity  
173 and information and yet ensure at the same time that we speak  
174 to privacy and civil-liberties protections.

175           I think it is also important that we don't take any  
176 actions that would inadvertently hinder the private-sector  
177 development of cybersecurity technology or create new network  
178 vulnerabilities, and that is why I am pleased to see that  
179 both public and private sectors are working together on these

180 issues and that the FCC's CSRIC unanimously endorsed  
181 voluntary industry-wide best practices to address the whole  
182 issue of botnets and domain name fraud and Internet route  
183 hijacking. So I think that they have done very good work and  
184 it is something that we need to take advantage of.

185         So today's hearing is really yet another opportunity for  
186 us to look at this slice that you can teach us about and that  
187 we weave that together all under the umbrella of really  
188 safeguarding some of the most important parts of our national  
189 infrastructure both public and private relative to  
190 cybersecurity.

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

192 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
193 Ms. {Eshoo.} With the time that I have remaining, I  
194 will yield it to Congresswoman Doris Matsui.

195 Ms. {Matsui.} Thank you very much, Ranking Member  
196 Eshoo, for yielding me time, and I would like to welcome our  
197 witnesses today, and I want to thank the chairman very much  
198 for having this hearing today and having explored some of  
199 these issues for the last month or so.

200 Communications networks are one of the many areas our  
201 Nation must protect to ensure safety and soundness. It will  
202 be important that data is protected in transit to cloud  
203 storage. A number of government agencies are using cloud  
204 services, so it is my hope that we can learn more from the  
205 early experiences.

206 I also believe that our subcommittee will have the  
207 ability to further promote information sharing on cyber  
208 threats. I will be interested in hearing from witnesses how  
209 information is being shared within the government and between  
210 the government and industry. There also seems to be a number  
211 of clearinghouses that are used to store information related  
212 to cyber threats. I will also be interested in hearing the  
213 relationship between those silos and industry and government  
214 sharing. Securing the supply chain will be of high  
215 importance.

216           We also need to consider that there might be some  
217 economic incentives that could encourage industry to explore  
218 ways to better address and defend against malware and  
219 botnets, and again, I welcome you all here today and I am  
220 looking forward to the testimony. Thank you very much.

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

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

|  
223           Mr. {Walden.} Thank you, and thanks for your service on  
224 the working group.

225           Now I recognize Representative Bono Mack for a minute,  
226 and then we will have Mr. Barton and Ms. Blackburn.

227           Mrs. {Bono Mack.} Thank you, Mr. Chairman.

228           In our two previous hearings on this issue, we have  
229 heard from representatives of the private sector and the  
230 communications industry who expressed real concern about the  
231 effects of heavy-handed new government regulation in this  
232 realm of cybersecurity. Onerous new regulations they say  
233 will likely fall haplessly behind existing technology and  
234 divert valuable resources away from security and towards  
235 regulatory compliance. Indeed, with so much information out  
236 there about the sophisticated and constantly evolving nature  
237 of cyber attacks, what the experts in the field have said  
238 they need most is the ability to better share information  
239 about existing cyber threats and the freedom to respond  
240 quickly to those threats.

241           Yesterday, Congresswoman Blackburn and I introduced the  
242 House companion to Senator John McCain's Secure IT Act, which  
243 first removes legal hurdles which prevent information sharing  
244 across the spectrum so that victims of cyber attacks can  
245 better work with each other to respond to cyber threats. I

246 believe that this approach, which empowers security experts  
247 to proactively address threats rather than reactively respond  
248 to them, is the best path forward.

249 I look forward to hearing from our witnesses today. I  
250 thank them for appearing before us, and I would like to yield  
251 back the balance of my time.

252 [The prepared statement of Mrs. Bono Mack follows:]

253 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
254           Mr. {Walden.} And I would recognize the gentlelady from  
255 Tennessee for a minute.

256           Mrs. {Blackburn.} Thank you, Mr. Chairman, and I want  
257 to thank your witnesses for being here.

258           You have heard us talk about the two previous hearings  
259 that we have done with industry, and of course, what they  
260 have pointed out is that there is no cookie-cutter approach  
261 that we can follow as we deal with what are very dangerous  
262 issues. One of the things that also has come out is that the  
263 federal government needs to be leading by example. If we  
264 want to provide assurance that there is going to be a pattern  
265 of security, this is going to be important for us to do, to  
266 lead by example.

267           Another thing that as we discuss this and how we are  
268 going to lead by example, I also want to hear about what you  
269 are doing to prioritize your R&D and how we are going to be  
270 able to work with the private sector in that vein. As  
271 Representative Bono Mack introduced, we introduced the Secure  
272 IT Act yesterday. This is going to focus on strong info-  
273 sharing components, making certain that we are addressing  
274 some increased penalties for criminals and priority and  
275 coordination of the federal research.

276           So thank you all, welcome, and yield back.

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

278 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
279 Mr. {Walden.} I now recognize Mr. Stearns for a minute.

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

281 Yesterday, Shawn Henry, the FBI's top cyber cop, told  
282 the Wall Street Journal that the current public and private  
283 approach to fending off hackers is unsustainable as computer  
284 criminals are simply too talented and defensive measures are  
285 too weak to stop them. He also expressed that companies need  
286 to make major, major changes in the way they use computer  
287 networks to avoid further to national security, and Mr.  
288 Chairman, I ask that the Wall Street Journal article be part  
289 of the record by unanimous consent.

290 Mr. {Walden.} Without objection.

291 [The information follows:]

292 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
293           Mr. {Stearns.} Today's hearing focuses on public-sector  
294 responses to threats to communications networks. I am  
295 interested to hear our witnesses' reaction to Mr. Henry's  
296 bleak outlook on our unsustainable model to cybersecurity as  
297 he says, ``unsustainable in that you never get ahead, never  
298 become secure, never have a reasonable expectation of privacy  
299 or security.''

300           As chairman of the Oversight and Investigations  
301 Subcommittee, I have held three cybersecurity hearings.  
302 Through these hearings and the ones held by our chairman  
303 today, I hope our committee can learn what we can do to make  
304 sure the good guys are winning again.

305           Thank you, Mr. Chairman.

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

307           \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
308 Mr. {Walden.} I thank the gentleman from Florida. Is  
309 anybody else seeking recognition here? I know Mr. Barton had  
310 wanted time but he is not here.

311 Now I will go to you, Mr. Waxman. We will return the  
312 balance of our time on this side and I now recognize the  
313 chairman emeritus, Mr. Waxman, for 5 minutes.

314 Mr. {Waxman.} Thank you very much, Mr. Chairman, for  
315 holding this hearing on cybersecurity.

316 It is important that we understand the government  
317 perspective. I am especially interested to learn the steps  
318 government agencies are taking to advance cybersecurity and  
319 secure the supply chain. I also welcome our expert from  
320 Carnegie Mellon.

321 The FCC, under the leadership of Chairman Genachowski  
322 and Admiral Barnett, has established a Communications  
323 Security, Reliability and Interoperability Council, or CSRIC,  
324 and today we can learn about CSRIC's recent recommendations  
325 promoting cybersecurity, as well as what other agencies are  
326 doing to promote best practices and information sharing.  
327 Efforts like CSRIC can help lead to adoption of best  
328 practices and voluntary codes of conduct by Internet service  
329 providers, software companies, manufacturers and security  
330 vendors.

331           But we also need to address the question of  
332   accountability. For example, what if one company fails to be  
333   as diligent as others in following best practices and, as a  
334   result, causes a cyber breach that rises to the level of a  
335   national concern? We need to explore whether reliance solely  
336   upon the private sector to ensure the security of  
337   communications networks across the country is sufficient, and  
338   what additional steps we might need to achieve enough  
339   accountability to best protect critical communications  
340   networks from cyber attacks.

341           We are hearing from industry that they want statutory  
342   exemptions from privacy and antitrust laws in order to  
343   facilitate information sharing. I have an open mind as we  
344   consider these issues. But this should be a two-way street.  
345   If industry wants exemptions from consumer protection laws,  
346   we have a right to ask for accountability that companies  
347   actually end up sharing information important for  
348   cybersecurity, do not abuse their privileges, and are held  
349   accountable.

350           There is a stronger case to be made for enabling sharing  
351   between the federal government and private industry, but we  
352   need to balance information sharing with sufficient privacy  
353   and civil-liberties protections. Further, we need to make  
354   sure that the federal agencies that engage in direct

355 information sharing with the private sector are civilian  
356 agencies, not intelligence or defense agencies.

357 I hope we will also discuss securing the communications  
358 supply chain. This is a growing potential threat, especially  
359 as we are now witnessing thousands of applications being  
360 loaded onto smart devices that connect to the public  
361 Internet. We should examine the best ways to address this.

362 I want to thank our panel of witnesses for their  
363 participation today and I look forward to hearing your  
364 testimony. I yield back the time.

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

366 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
367           Mr. {Walden.} The gentleman yields back the balance of  
368 his time. We will now proceed with our witnesses. We thank  
369 you all for being here and look forward to your comments.

370           We will start with Ms. Fiona Alexander, Associate  
371 Administrator, Office of International Affairs, National  
372 Telecommunications and Information Administration, NTIA, U.S.  
373 Department of Commerce. That is a mouthful. We are glad you  
374 are here today and we look forward to hearing from you. And  
375 just a heads-up for everybody, these microphones, you have to  
376 get pretty close to for people to hear, and make sure it is  
377 lit.

|  
378 ^STATEMENTS OF FIONA ALEXANDER, ASSOCIATE ADMINISTRATOR,  
379 OFFICE OF INTERNATIONAL AFFAIRS, NATIONAL TELECOMMUNICATIONS  
380 AND INFORMATION ADMINISTRATION (NTIA), U.S. DEPARTMENT OF  
381 COMMERCE; ADMIRAL JAMES BARNETT, JR. (RET.), CHIEF, PUBLIC  
382 SAFETY AND HOMELAND SECURITY BUREAU, FEDERAL COMMUNICATIONS  
383 COMMISSION (FCC); ROBERT HUTCHINSON, SENIOR MANAGER FOR  
384 INFORMATION SECURITY SCIENCES, SANDIA NATIONAL LABORATORIES;  
385 GREGORY SHANNON, CHIEF SCIENTIST, COMPUTER EMERGENCY  
386 READINESS TEAM, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE  
387 MELLON UNIVERSITY; AND ROBERTA STEMPFLEY, ACTING ASSISTANT  
388 SECRETARY FOR CYBER SECURITY AND COMMUNICATIONS, DEPARTMENT  
389 OF HOMELAND SECURITY

|  
390 ^STATEMENT OF FIONA ALEXANDER

391 } Ms. {Alexander.} Thank you very much. It is a very  
392 long name. So good morning, Chairman Walden, Ranking Member  
393 Eshoo and members of the subcommittee. Thank you for this  
394 opportunity to testify on behalf of the Department of  
395 Commerce's NTIA regarding cybersecurity.

396 NTIA, as you know, is the President's principal advisor  
397 on telecommunications and information policy matters and is  
398 the executive branch expert on issues relating to the

399 Internet's Domain Name System, a critical component of the  
400 cyber infrastructure. NTIA supports a multi-stakeholder  
401 approach to the coordination of the DNS to ensure long-term  
402 viability of the Internet. Working with other stakeholders,  
403 NTIA develops policies and takes actions to preserve an open,  
404 interconnected global Internet that supports continued  
405 innovation and economic growth, investment and the trust of  
406 its users. This multi-stakeholder model of Internet  
407 policymaking convening the private sector, civil society and  
408 government to address issues in a timely and flexible manner,  
409 has been responsible for the past success of the Internet and  
410 is critical to its future.

411         The authenticity of DNS data is essential to the  
412 security of the Internet as it is vital that users reach  
413 their intended destinations and are not unknowingly  
414 redirected to fraudulent and malicious websites. This is one  
415 of the primary objectives motivating NTIA's efforts to secure  
416 the DNS and what I will specifically address today.

417         The early DNS, while exceptional in many ways, lacked  
418 strong security mechanisms. Over time, hackers and others  
419 have found more and more ways to exploit vulnerabilities in  
420 the DNS protocol. That put the integrity of DNS data at  
421 risk. These vulnerabilities increase the likelihood of  
422 certain DNS-related cyber attacks which can lead to identify

423 theft and other security compromises.

424           In response to these risks, the Internet Engineering  
425 Task Force developed a suite of specifications for securing  
426 information provided by the DNS called Domain Name System  
427 Security Extensions, or DNSSEC. DNSSEC provides an  
428 additional layer of security to DNS by authenticating the  
429 origin of the DNS data and verifying its integrity while it  
430 moves across the Internet.

431           In 2008, NTIA undertook a multi-stakeholder public  
432 consultation process regarding whether and how DNSSEC should  
433 be deployed at the authoritative route, the top level of a  
434 DNS hierarchy for which NTIA continues to have historical  
435 oversight. In response to the public notice, NTIA received  
436 overwhelming support from the international Internet  
437 community to move forward as soon as possible. Over the next  
438 year and a half, NTIA, drawing upon the input and expertise  
439 of technical experts from around the world, and working close  
440 with NIST, our sister agency at Commerce, as well as our root  
441 zone management partners, VeriSign and ICANN, moved to fully  
442 deploy DNSSEC at the root in July 2010.

443           DNSSEC essentially gives a tamper-proof seal to the  
444 address book of the Internet, similar to a wax seal on an  
445 envelope. For example, I can send you a letter in an  
446 envelope, but when you receive the envelope, you don't know

447 if it was tampered with, but if I use my seal on some wax  
448 across the envelope's closure, then you know two things: the  
449 letter wasn't tampered with in transit, which means there is  
450 data integrity, and that I was the one who sent it, because  
451 you recognize my stamp, which is data origin authentication.  
452 If you know that I always seal my letters and you receive a  
453 letter from me that isn't sealed or the seal is broken, you  
454 know that a bad guy or a man in the middle could have opened  
455 the sealed envelope and replaced the contents. You can throw  
456 it away because you know it is a fake. DNSSEC information is  
457 like the letter in the envelope. DNSSEC gives that  
458 information a seal that verifies and authenticates it.

459         DNSSEC deployment at the authoritative root was an  
460 important step toward protecting the integrity of DNS data  
461 and mitigating attacks such as cache poisoning, which allows  
462 the hacker to redirect traffic to fraudulent sites and other  
463 data modification threats. This effort marks significant  
464 progress in making the Internet more robust and secure as it  
465 provides a tool to facilitate greater user confidence in the  
466 online experience so that when someone visits a particular  
467 website, whether it be a bank, a retailer or a doctor, they  
468 are not seeing a spoofed copy that cyber criminals can use to  
469 perpetuate identify theft or other crimes using the DNS.

470         In helping to deploy DNSSEC at the root zone, NTIA

471 sought to facilitate greater DNSSEC deployment throughout the  
472 Internet. If we are to maintain trust in the Internet, then  
473 we must support further DNSSEC deployment. Governments as  
474 well as other stakeholders must continue to support the  
475 deployment and development of DNSSEC-related software, tools  
476 and other products and services. As we explore issues  
477 affecting Internet space, we should take all appropriate  
478 steps to ensure that DNSSEC use and adoption continues to  
479 grow.

480 In the coming months, NTIA, working as a part of the  
481 Department of Commerce's Internet Policy Task Force, will be  
482 looking for opportunities to launch further multi-stakeholder  
483 processes aimed at enhancing the security and stability of  
484 the DNS as well as broader cybersecurity efforts.

485 Thank you again for the opportunity to testify, and I  
486 will be happy to answer any questions.

487 [The prepared statement of Ms. Alexander follows:]

488 \*\*\*\*\* INSERT A \*\*\*\*\*

|  
489           Mr. {Walden.} Ms. Alexander, we appreciate your  
490 comments and we look forward to the questions.

491           Admiral, we are delighted to have you here today,  
492 Admiral James Barnett, Jr. (Ret.), Chief, Public Safety and  
493 Homeland Security Bureau, Federal Communications Commission,  
494 the FCC. Welcome, and we look forward to your comments.

|  
495 ^STATEMENT OF JAMES BARNETT, JR.

496 } Admiral {Barnett.} Thank you, Chairman Walden, Ranking  
497 Member Eshoo and all the distinguished members of the  
498 subcommittee. I really appreciate the opportunity to come  
499 and talk to you on this important topic of cybersecurity, and  
500 I am particularly pleased to be able to testify with these  
501 experts and especially my colleagues from DHS and Commerce  
502 with whom we work very closely on cybersecurity matters.

503 Cybersecurity threats are a real and present danger to  
504 our current economy and wellbeing. No one would tolerate the  
505 level of criminality, thievery, vandalism or invasion of  
506 privacy that we experience today if it were done in the  
507 physical world, and we really can no longer afford to  
508 tolerate it in cyberspace.

509 The approximately 40,000 autonomous systems or networks  
510 on which the Internet is built are largely commercial or  
511 privately owned. Commercial communications providers are  
512 therefore the first line of defense against cyber threats and  
513 always will be. Earlier this month, on March 7th, the  
514 subcommittee heard from cybersecurity experts in the  
515 communication industry about how hard they are working  
516 against those threats, yet if those efforts alone were

517 sufficient to thwart cyber threats, I don't think we would be  
518 here today. To be successful in battling cyber threats, we  
519 must work together collectively, industry and the public  
520 sector.

521       As the Nation's expert agency on communications, we have  
522 always been concerned with the security and reliability of  
523 networks. The FCC has a long history of working on network  
524 reliability and security with the companies that operate the  
525 core of the Internet. We have constituted a Cybersecurity  
526 and Communications Reliability Division in the Public Safety  
527 and Homeland Security Bureau. These are our cyber experts  
528 who among other duties coordinate the work of our current  
529 federal advisory committee, the Communications Security,  
530 Reliability and Interoperability Council, CSRIC which you  
531 mentioned before. CSRIC is now made up of over 50 industry  
532 leaders from the private sector and the federal government  
533 including cyber experts from DHS and NIST and a veritable  
534 all-star cast of Internet pioneers and world-class  
535 cybersecurity experts that are working on the council and the  
536 working groups.

537       And I am pleased to report that last week, CSRIC  
538 approved voluntary industry-based recommendations addressing  
539 three crucial problems. These recommendations are not simply  
540 a set of reports that will adorn bookshelves. Numerous ISPs

541 including Comcast, Verizon, AT&T, Time Warner, Sprint, Cox,  
542 T-Mobile, Frontier and CenturyLink have already pledged to  
543 implement the CSRIC recommendations as they apply to their  
544 respective networks. This means that these new cybersecurity  
545 measures will soon be protecting a significant majority of  
546 American Internet users.

547 First, CSRIC recommended that ISPs adopt a voluntary  
548 code of conduct to provide critical security to Internet  
549 users to fight botnets, which can steal personal information.  
550 We refer to it as the anti-bot code, a code that specifically  
551 addresses privacy of the end user.

552 Second, CSRIC examined Internet route hijacking, which  
553 can occur due to the lack of verification between networks.  
554 Internet route hijacking can endanger valuable intellectual  
555 and private property and jeopardize our national security.  
556 In 2010, traffic to 15 percent of the world's Internet  
557 destinations was diverted through Chinese servers for  
558 approximately 18 minutes. CSRIC recommended that ISPs embark  
559 upon a path toward implementation of secure routing  
560 protocols, or secure BGP, to minimize route hijacking. This  
561 would include the establishment of a secure, authoritative  
562 database of Internet address blocks to be used and checked by  
563 ISPs

564 CSRIC's third area of action is the Domain Name System,

565 DNS, which Ms. Alexander just mentioned. DNS can be thought  
566 of as the telephone book for the Internet, one that can be  
567 spoofed and can lure exposure of private information. DNSSEC  
568 can correct this problem. It was designed with privacy in  
569 mind. CSRIC endorsed DNSSEC implementation by ISPs and  
570 industry-wide adoption of the standard to help prevent  
571 unsuspecting Internet users from being sent to fraudulent  
572 websites.

573         These voluntary initiatives stand as an example to the  
574 world of how to promote cybersecurity while preserving the  
575 core characteristics of the Internet, which have fueled the  
576 broadband economy's growth and success. These efforts focus  
577 on ISPs but they dovetail into broader cybersecurity efforts  
578 by NIST and DHS which must address the larger information  
579 technology community. We will continue to work with  
580 industry, the multi-stakeholders and federal partners on  
581 voluntary industry-based solutions. We will carefully guard  
582 the reliability and security of all communications networks.  
583 Thank you.

584         [The prepared statement of Admiral Barnett follows:]

585 \*\*\*\*\* INSERT B \*\*\*\*\*

|  
586           Mr. {Walden.} Admiral, thank you very much. We  
587 appreciate your testimony, even if it is ever more disturbing  
588 the more we hear.

589           With that, we will now go to Mr. Hutchinson, Senior  
590 Manager for Information Security Sciences at Sandia National  
591 Laboratories. Thanks for all the work you and your team do  
592 out there at Sandia, and we appreciate your being here today  
593 to further enlighten us about the threat that we face and how  
594 we might deal with it appropriately, so please go ahead.

|  
595 ^STATEMENT OF ROBERT HUTCHINSON

596 } Mr. {Hutchinson.} Good morning. Chairman Walden and  
597 Ranking Member Eshoo and the distinguished members of the  
598 committee, thank you for inviting me to testify before you  
599 today. I am Bob Hutchinson, Senior Manager for Information  
600 Security Sciences at Sandia National Laboratories. Sandia is  
601 a federally funded research and development center for the  
602 Department of Energy. DOE makes its significant investment  
603 in Sandia's cybersecurity capabilities available to the  
604 Departments of Defense and Homeland Security as well as other  
605 government agencies and non-federal entities.

606 I have been working to secure critical government  
607 communications systems both as a researcher and as an  
608 implementer for over 25 years, and today's testimony is based  
609 on that experience. The most important lesson that I have  
610 learned in my career is that computer systems can never be  
611 fully trusted and can never be proven free of compromise, so  
612 we must focus on finding ways to conduct business, even  
613 critical business, on machines that are presumed to be  
614 infected. Our focus should be on accomplishing our goals and  
615 not on building and maintaining perfect computers and  
616 computer networks.

617 I would like to suggest four specific shifts in current  
618 national approach to cybersecurity. Each of these  
619 suggestions implies a role for the government and a role for  
620 the private sector. My intention is to highlight the  
621 strengths of each of these communities and to find ways that  
622 they can reinforce each other's interests.

623 Number one: In recent years, the Nation's cybersecurity  
624 approach has shifted to an almost exclusive focus on data  
625 theft. While this trend has been going for a number of years  
626 it understandably worsened in the aftermath of the Wikileaks  
627 intelligence theft. Our best security analysts are being  
628 taught to focus their attention on indications that sensitive  
629 data is leaving our networks headed into enemy hands. While  
630 data theft is a critical problem for the government and for  
631 the private sector, I believe that our Nation has diverted  
632 too many resources away from an equally, if not more  
633 important issue: malicious data modification. As much as I  
634 worry about the theft of sensitive data and U.S. intellectual  
635 property, my greater fear is that an attacker will alter our  
636 data and affect our decision processes. This form of attack  
637 has not only economic consequences but can also impact public  
638 safety and confidence. My staff and I focus much of our  
639 research on these scenarios. The security community must  
640 continue to worry about data theft but not to the detriment

641 of other cyber attack goals. The government should increase  
642 focused research and development investment on preserving  
643 data integrity.

644         Number two: We tend to view the stacks of mobile  
645 devices and networking components that arrive in U.S. ports  
646 as pristine. When we discover a compromise, we strive to  
647 return these devices to their original settings. This is a  
648 fundamentally flawed security model. We don't have any idea  
649 whether our devices have been precompromised during design,  
650 manufacture or distribution. We call this a supply chain  
651 attack. As an unclassified example, a few years ago a major  
652 hard-drive manufacturer was discovered to have shipped brand-  
653 new hard drives with malware preinstalled. The government,  
654 in part through Sandia, has been addressing these supply  
655 chain attacks for over three decades. The commercial  
656 companies share this risk with the government. The  
657 government can help industry by informing commercial  
658 companies of our lessons learned and helping those companies  
659 use their existing supply relationship to begin addressing  
660 this problem where it will have the greatest impact directly  
661 within the company's own supply chains.

662         Number three: It is not enough that the government  
663 shares details of cybersecurity incidents with the community  
664 of interest. It also needs to develop and share strategies.

665 Cybersecurity is more like a game of poker than a reaction  
666 not a natural disaster. Simply sharing data without rules  
667 and strategies prevents us from working together effectively.  
668 For instance, careful coordination of our activities can  
669 cause an adversary to reveal his identity.

670 Finally, number four: The most consistent cybersecurity  
671 message across government and industry is that our Nation has  
672 a profound shortage of qualified cybersecurity experts.  
673 There are many efforts to educate, train and certify.  
674 Degrees and certifications are not enough. Cybersecurity is  
675 a new field that lacks scientific and engineering rigor. The  
676 best people in this field learn through practice and  
677 apprenticeship. They use judgment that is based on years of  
678 experience. The Department of Energy began to address this  
679 issue over 10 years ago when they asked Sandia to build a  
680 program that is more like a medical residency than a trade  
681 certification. Many of the people who have participated in  
682 this program have become national leaders in securing  
683 emerging technologies such as mobile device networks and  
684 cloud services. This investment has yielded greater returns  
685 than any other program in which I have been involved.  
686 Expanding this model so that all U.S. cybersecurity  
687 professionals learn through a residency would result in  
688 enormous gains for national security.

689 I would like to thank you for this opportunity to  
690 testify, and I look forward to your questions.

691 [The prepared statement of Mr. Hutchinson follows:]

692 \*\*\*\*\* INSERT C \*\*\*\*\*

|  
693           Mr. {Walden.} Thank you, Mr. Hutchinson. We appreciate  
694 your disturbing testimony.

695           Now we are going to go to Mr. Greg Shannon, the Chief  
696 Scientist, Computer Emergency Readiness Team, Software  
697 Engineering Institute at Carnegie Mellon University. Dr.  
698 Shannon, thank you for being here. We look forward to your  
699 testimony.

|  
700 ^STATEMENT OF GREGORY SHANNON

701 } Mr. {Shannon.} Thank you, Chairman Walden, Ranking  
702 Member Eshoo and distinguished committee members. I am  
703 honored to testify before you today on cybersecurity and  
704 communication networks. I am the Chief Scientist for the  
705 CERT cybersecurity program at the Software Engineering  
706 Institute, which is a Department of Defense FFRDC operated by  
707 Carnegie Mellon University.

708 CERT was created in 1988 by DARPA in response to the  
709 moratorium incident and now we are a national asset for  
710 cybersecurity with 250 staff tackling our Nation's technical  
711 cybersecurity challenges. At CERT, we recognize the long-  
712 term challenges as we confront the threats, deliver pragmatic  
713 solutions and consider the technical roles for the private  
714 and public sectors. We see two important policy  
715 opportunities with long-term benefits.

716 First is to broadly promote the use of scientifically  
717 and operationally validated policies, best practices,  
718 technologies, standards, products, etc. Validated  
719 capabilities should trump unvalidated ones.

720 Second is to actively enable controlled access to real  
721 high-fidelity operational data for research. Good results

722 require good data as part of a long-term solution. Rigor and  
723 data are the foundations of many successful technical public-  
724 private partnerships such as National Centers for Disease  
725 Control, the National Highway Transportation Traffic Safety  
726 Administration and the National Transportation Safety Board.  
727 Trusted public-private collaborations represent our mature  
728 adoption of technology and are an important step for  
729 cybersecurity to become a distinguishing capability for our  
730 Nation.

731         Understanding today's cyber threats to our  
732 communications networks is about more than war stories,  
733 anecdotes and scare tactics. Adversaries can combine supply  
734 chain and operational vulnerabilities in hardware, software,  
735 data and humans to create multitudes of attack strategies.  
736 Policies should address the root causes of our cyber threats  
737 and not just the immediate symptoms. Otherwise our  
738 adversaries will merely use another combination of what we  
739 haven't yet explicitly blocked, which is a continuously  
740 losing battle for cybersecurity.

741         For decades, the public sector, often in partnership  
742 with CERT, has addressed the technical symptoms and root  
743 causes of cybersecurity threats and attacks together. At  
744 CERT, we help millions of programmers write secure software  
745 to address the root cause of vulnerable software. We help

746 agencies protect critical information, critical  
747 infrastructure operated by hundreds of private companies to  
748 address the challenges of responding to active attacks with  
749 potentially serious consequences. Using our decade-long work  
750 on resiliency management and smart grid maturity models, we  
751 are helping the Department of Energy, DHS and the White House  
752 with the Electricity Sector Cybersecurity Risk Management  
753 Maturity Project. Such work will remove core vulnerabilities  
754 and decrease the impact of attacks.

755       To better understand cybersecurity problems and  
756 solutions, the science of cybersecurity is now broadly  
757 endorsed and funded by key federal science and technology  
758 agencies including the Department of Energy. Policymakers  
759 can assist the research community by explicitly requesting  
760 cybersecurity innovations and practices that are  
761 scientifically and operationally valid. Furthermore,  
762 policymakers can request data owners, public or private, and  
763 the research organizations who can diligently use the data to  
764 provide appropriate access to high-fidelity operational data.  
765 Only with such data can cybersecurity researchers learn  
766 leading attack indicators, identify underlying principles and  
767 evaluate solutions.

768       Another role for the public sector is to improve the  
769 trust required for effective cyber attack preparation and

770 response by clarifying public and private roles in  
771 cybersecurity, especially with respect to information  
772 sharing. Consider establishing one or more national  
773 repositories of operational cybersecurity data for research  
774 purposes. Access to such a repository would enable cyber  
775 research to reach new levels. Sharing cyber data with strong  
776 privacy controls would engender research that can look more  
777 globally and more predictably at the problem, especially in  
778 the long term.

779         In conclusion, every day we at CERT see the value of  
780 trust, rigor and data in helping mitigate cyber  
781 vulnerabilities, threats and attacks. We look forward to the  
782 day when our Nation can handle cybersecurity threats and  
783 attacks with the same efficiency and effectiveness as our  
784 Nation's response to the H1N1 health crisis. Then  
785 cybersecurity will truly be a distinguishing national  
786 capability alongside others such as our ability to innovate.  
787 Thank you.

788         [The prepared statement of Mr. Shannon follows:]

789 \*\*\*\*\* INSERT D \*\*\*\*\*

|  
790           Mr. {Walden.} Doctor, thank you. We appreciate your  
791 testimony.

792           And our final witness on the panel is Roberta Stempfley,  
793 Acting Assistant Secretary for Cybersecurity and  
794 Communications, Department of Homeland Security. We are  
795 delighted to have you here this morning and we look forward  
796 to your testimony.

|  
797 ^STATEMENT OF ROBERTA STEMPFLEY

798 } Ms. {Stempfley.} Thank you very much, Chairman Walden  
799 and Ranking Member Eshoo. As you said, I am with the  
800 Department of Homeland Security. I have two decades of  
801 experience as a public servant working both in the Defense  
802 Department for 18 years and now almost two years at the  
803 Department of Homeland Security, and it is certainly a  
804 privilege for me to have the opportunity to come and speak to  
805 you today about the efforts that the Department of Homeland  
806 Security has that support the cybersecurity of our important  
807 communications networks.

808 As you know, the private sector owns most of the  
809 national infrastructure in the communications environment and  
810 as such, protecting the communications networks is not  
811 something the federal government can or should do alone.  
812 There is no silver bullet to cybersecurity, as my esteemed  
813 panel colleagues have indicated. There is not a single tool,  
814 a single technique nor a single organization who is capable  
815 or accountable or responsible for delivering cybersecurity to  
816 the communications networks. But access to reliable and  
817 consistent communications is essential to maintaining the  
818 Nation's health, safety, economy and public confidence.

819 Protection of communications infrastructure from this  
820 range of threats, national disasters, terrorism and  
821 cybersecurity, is of the highest priority to the Department  
822 of Homeland Security, and this communications infrastructure  
823 is complex. It is a system of systems with multiple  
824 ownerships and multiple interconnection points. It involves  
825 wireline, wireless, satellite, broadcast capabilities and  
826 serve the transport and enable this Internet that we live,  
827 play and function on.

828 The Office of Cybersecurity and Communications in the  
829 Department's National Protection and Programs Directorate is  
830 designated the federal entity to lead the coordination with  
831 both the communications and information technology sectors of  
832 critical infrastructure. We work closely with these partners  
833 and ensure robust and resilient communications throughout the  
834 Nation.

835 Within this Office of Cybersecurity and Communications,  
836 we have an organization called the National Communications  
837 System, which is the lead for the communications sector. It  
838 leads government-industry coordination critical in the  
839 planning, initiation, restoration and reconstitution of  
840 national security emergency preparedness service and  
841 facilities. The National Cybersecurity Division is  
842 responsible for leadership in the information technology

843 sector and responsible for major cybersecurity programs that  
844 we will be speaking of today.

845         Additionally, we have the Office of Emergency  
846 Communication, which supports and promotes the ability in  
847 emergency responders and government officials to communicate  
848 in the event of a disaster. The Office of Emergency  
849 Communication's focus is on that interoperable and operable  
850 emergency communications nationwide.

851         All of these organizations and others come together in  
852 an operation center called the National Cybersecurity  
853 Communication and Integration Center. It houses the National  
854 Coordinating Center for Communications, a part of the  
855 National Communications System, the U.S. Computer Emergency  
856 Readiness Team, a part of the National Cybersecurity  
857 Division, as well as other partners from industry and across  
858 the federal government including members of the  
859 Communications, Information Sharing and Analysis Center. Our  
860 collective efforts tie into the DHS-wide collaboration and  
861 extend our partnership with federal, state, local governments  
862 and the private sector, and together we work under  
863 orchestration to negate threats to the communications  
864 infrastructure and to build strategies for future success.

865         Protection of that communications infrastructure is  
866 conducted in this holistic fashion and encompasses physical

867 and cyber threat strategies. Partnerships are key and very  
868 important as is two-way information sharing. We have this  
869 information sharing real time on the floor, as I indicated,  
870 where 5,200 alerts were released by U.S. CERT to our partners  
871 over the course of the last year. The Department employs  
872 mechanisms to ensure that the sensitive propriety information  
873 shared with us from industry is protected and that privacy  
874 and civil liberties are upheld. It is industry's willingness  
875 to share this information on a voluntary basis that speaks to  
876 the strong trust between DHS and its private-sector partners  
877 as we work forward in this situation.

878 I spoke to that Communications Information Sharing and  
879 Analysis Center. There are information sharing and analysis  
880 centers within each sector. They are sector specific. And  
881 in that sector, we have 56 private-sector partners that were  
882 the first operations entity from the private sector on the  
883 floor of the National Cybersecurity Communications  
884 Integration Center.

885 In addition, in the Department, the Secretary serves as  
886 the executive agent supporting the President's National  
887 Security Technology Advisory Committee. This committee is  
888 comprised of up to 30 chief executives from industries like  
889 network service providers, telecommunications, information  
890 technology, finance and aerospace companies. The NSTAC makes

891 recommendations to the President on strategies and practices  
892 to secure vital communications links through events and  
893 crises. We also have worked in partnership on communication  
894 sector supply chain threats, an item of interest to the  
895 committee today.

896         Given the increasing use of technologies such as  
897 smartphones by first responders, there are real innovations  
898 available in that situation and the Public Safety Broadband  
899 Network that this committee was so integral in establishing  
900 must be secure and reliable so that emergency responders can  
901 be assured that sensitive information is protected and  
902 accurate. DHS is committed to working with all of our  
903 public- and private-sector partners today including NTIA and  
904 the FCC, who I am pleased to be with on the panel today, to  
905 ensure we secure the National Public Safety Broadband Network  
906 through this holistic approach with equal emphasis on  
907 protecting confidentiality, integrity and availability.

908         Thank you again for this opportunity to testify, and I  
909 am pleased to answer your questions.

910         [The prepared statement of Ms. Stempfley follows:]

911         \*\*\*\*\* INSERT E \*\*\*\*\*

|  
912           Mr. {Walden.} Thank you, Ms. Stempfley. We appreciate  
913 your comments. We were just talking here about, as you  
914 described, the center out here, about maybe the subcommittee  
915 coming out to take a look at some point.

916           Ms. {Stempfley.} We welcome you. Any time you would  
917 like, we would more than honored to have you out there and  
918 show you the span of activity that goes on in that center.  
919 As I said in my comments, it is a place where government and  
920 industry come together. We have representative not just from  
921 the communications sector but from the information technology  
922 sector, from the financial sector and from other partners on  
923 that floor as well as partners across government from the  
924 intelligence community and others.

925           Mr. {Walden.} All right. Thank you.

926           My first question would be to you. The Department of  
927 Commerce's Economic Development Administration recently  
928 suffered a cyber attack that has left the agency without  
929 network connectivity for several weeks, I am told. Could you  
930 elaborate on that situation and what DHS has been doing to  
931 address it, and has it been resolved?

932           Ms. {Stempfley.} The Department of Homeland Security  
933 has responsibility for protection and defense of the federal  
934 executive civilian branch including the Department of

935 Commerce includes responsibilities for supporting the  
936 Department when they had a compromise of the nature that you  
937 are describing at the EDA. We have individuals on the ground  
938 with Commerce to support EDA in the reconstitution of their  
939 network and are building it in a way that is supportive of  
940 increased security and the meeting of the federal standards  
941 that are initiated both by the Department and the Federal  
942 Information Security Management Act.

943 Mr. {Walden.} So are they still offline?

944 Ms. {Stempfley.} I am personally not sure, sir, at the  
945 moment but we would be happy to follow up with you on that.

946 Mr. {Walden.} Any idea where the attack came from?

947 Ms. {Stempfley.} I don't know attribution in this  
948 situation. Attribution is generally the responsibility of  
949 law enforcement and the intelligence community. We are  
950 responsible for protection and mitigation measures, and I am  
951 happy to come back with our partners from Commerce.

952 Mr. {Walden.} That seems pretty major if it has been  
953 offline for several weeks.

954 There has been a resounding call for increased consumer  
955 education when it comes to cybersecurity, and this is kind of  
956 for everybody here. However, a report released earlier this  
957 month by Trust Wave showed that after studying more than 300  
958 data breaches in 2011, nearly 5 percent of the passwords on

959 the compromised networks were variations of the word  
960 ``password.'' So if end users cannot even wrap our heads  
961 around not using the word ``password'' as a password, how can  
962 we as policymakers form a better understanding of a complex  
963 topic like route hijacking? Does anybody want to take that  
964 one quickly?

965       Mr. {Shannon.} At Carnegie Mellon University, there is  
966 a large number of researchers studying how to make security  
967 and privacy usable and it is turning out to be very daunting.  
968 The password research has shown that people do reuse  
969 passwords. When you get populations of passwords together,  
970 it creates a vulnerability. So it becomes clear that  
971 individuals--it is difficult for us to rely on individuals to  
972 be the foundation of security.

973       Mr. {Walden.} I want to ask a different question of  
974 you, Dr. Shannon. Some of the vulnerabilities in compromised  
975 systems persist despite common knowledge among computer  
976 programmers the problem. For example, SEQUEL, the structured  
977 query language injection, has been one of the most common  
978 vectors for database attacks for years, I am told. How do we  
979 change the culture at coding to ensure the security is more  
980 of a focus?

981       Mr. {Shannon.} One is by providing explicit guidelines,  
982 which we have been doing for the last 10 years. SEQUEL is

983 not a language that we have tackled. We have been focused on  
984 C++ and Java and the C programming language. Part of the  
985 challenge is that we do not control where the programs are  
986 written so they may be written offshore under economically  
987 stressed and time constraints. So it is a challenge of  
988 improving the general practice and by providing coding  
989 standards is our step in that direction.

990 Mr. {Walden.} All right. Thank you.

991 Mr. Hutchinson, you recommended, I think, four points of  
992 things we should look at and talked about the supply chain  
993 issues and this notion of precompromises of hardware with  
994 malware installed. Are there more examples of that we should  
995 be aware of in this setting?

996 Mr. {Hutchinson.} In this setting, I can't cover. The  
997 examples I am aware of are classified. But, you know, I  
998 would very much welcome a classified discussion on that  
999 topic.

1000 Mr. {Walden.} Could you speak more about the malicious  
1001 data modification issues in this setting? What does that  
1002 mean? What are we seeing as examples?

1003 Mr. {Hutchinson.} So just for context, when you--when  
1004 an event occurs on a network, the most normal thing for an  
1005 analyst to do is to look for the exfiltration of data from  
1006 that network, to analyze malicious code to determine whether

1007 it is stealing data from the network and pointing it in the  
1008 direction of the adversary. The malicious modification would  
1009 be something that the compromise leaves behind that alters  
1010 the data, changes the nature of the data, changes emails,  
1011 things like that.

1012 Mr. {Walden.} I see. Okay. And a question I have  
1013 asked all the panels we have had before, sort of in with the  
1014 Hippocratic oath, first, do no harm. Do you each, could you  
1015 real quickly just say what is the one caution you could offer  
1016 as we promulgate legislation? Ms. Alexander, what shouldn't  
1017 we do?

1018 Ms. {Alexander.} I think it is important that as you  
1019 consider ways to deal with this important issue, there is a  
1020 grounding and understanding of how the network actually works  
1021 so that the rules that are developed don't inadvertently  
1022 undercut some of the other activities.

1023 Mr. {Walden.} All right. Admiral Barnett?

1024 Admiral {Barnett.} So I think it is important to make  
1025 sure that we don't cut off this engine of innovation, that as  
1026 we move forward that we continue to have that openness. But  
1027 I would also say that as you do it, you have to look at the  
1028 performance metrics. Are the things that we are doing  
1029 actually having some effect? We have to have data driven to  
1030 make sure that we are actually doing some good.

1031 Mr. {Walden.} Mr. Hutchinson?

1032 Mr. {Hutchinson.} So there are some very strong  
1033 relationships in helping this problem like the relationship  
1034 between DHS and NSA. Anything that would harm that  
1035 relationship I think would be hurtful to the government.

1036 Mr. {Walden.} Keeping open communication?

1037 Mr. {Hutchinson.} Yes, that communication and the  
1038 relationship between the NSA and applying classified  
1039 approaches to this otherwise unclassified problem I think is  
1040 extraordinarily valuable.

1041 Mr. {Walden.} Okay. Dr. Shannon?

1042 Mr. {Shannon.} I think we need to protect innovation,  
1043 as the admiral mentioned. There is a balance between too  
1044 little security that allows for the loss of intellectual  
1045 property and then onerous security that imposes a tax on  
1046 innovation in the long term and makes us no better than other  
1047 countries that are more restrictive in how their citizens  
1048 behave, so I think there is a real balance to maintain there  
1049 to promote innovation.

1050 Mr. {Walden.} All right. Ms. Stempfley?

1051 Ms. {Stempfley.} As several individuals have  
1052 identified, there are relationships and partnerships and  
1053 multiple organizations that are involved, and those  
1054 relationships must equally be sustained and we must continue

1055 to empower the multiple organizations that are involved here.

1056 Mr. {Walden.} Thank you all very much.

1057 Now I turn to Ms. Eshoo for questions.

1058 Ms. {Eshoo.} Thank you, Mr. Chairman, and to each of  
1059 the witnesses, thank you. Excellent testimony. There was a  
1060 group of students that were here, and you are facing this  
1061 way, but I couldn't help but notice that they all left en  
1062 masse, and I thought we have either scared the hell out of  
1063 them or bored them. I don't know. I think that that might  
1064 apply to us as well because there are so many moving parts to  
1065 this.

1066 I have a whole list of very specific questions but I  
1067 want to set those aside. I will put them in writing to you,  
1068 and I don't think we need to ask for unanimous consent, no,  
1069 because members can ask questions in writing of the  
1070 witnesses.

1071 When we look at the whole issue of cybersecurity, it is  
1072 my understanding that 5 percent responsibility in the public  
1073 sector, the government. Ninety-five percent of this rests  
1074 with the private sector. Now, CSRIC has come up with some  
1075 recommendations. Both the chairman and myself and I think  
1076 that other members have referenced it. Maybe some of you did  
1077 in your testimony. But I want to ask you the following  
1078 question, and I appreciate the rather deep dives that you

1079 have done on your specific area of expertise and what your  
1080 observations are. But for each one of you, on the 5 percent,  
1081 which is the government, what is the top recommendation that  
1082 you would make to us that we need to take into consideration  
1083 that will help remake the landscape into a very smart one to  
1084 address the threats that come to us relative to cybersecurity  
1085 in the government. Ms. Alexander, I don't have a lot of  
1086 time. We have got, like, 3 minutes for five of you.

1087 Ms. {Alexander.} Sure. I think in addition to this  
1088 idea of continuing innovation and voluntary codes of conduct,  
1089 government is very powerful as a user and so we can set  
1090 examples and we influence procurement patterns. I think that  
1091 is one of the most powerful things that we can do as  
1092 government.

1093 Mr. {Eshoo.} Excellent. Thank you very much.

1094 Admiral, thank you for your wonderful work.

1095 Admiral {Barnett.} Thank you, ma'am. So I think  
1096 continuing to seek voluntary and industry-based solutions is  
1097 the bedrock, incentivizing that and looking for that, and  
1098 then obviously as almost every person mentioned in your  
1099 openings, we really have to tackle the supply chain.

1100 Ms. {Eshoo.} Thank you.

1101 Mr. {Hutchinson.} So maintaining opt-in alternatives  
1102 for industry to seek government's help in incentivizing those

1103 I think is critical, and the supply chain is an area that  
1104 will become increasingly problematic, and I think we need to  
1105 work hard with industry to take the government know-how.

1106 Mr. {Shannon.} I would say trust is--

1107 Ms. {Eshoo.} Excuse me. I am sorry, Dr. Shannon. Let  
1108 me get back to you, Mr. Hutchinson. Are you suggesting that  
1109 practices on the public side is something that the private  
1110 side can gain a great deal from, or is it the other way  
1111 around?

1112 Mr. {Hutchinson.} Yes, this is a problem that the  
1113 private side does not understand well and the government  
1114 understands very well yet the private side has the problem to  
1115 the same degree that the government does, so this is a great  
1116 opportunity for the government to inform.

1117 Ms. {Eshoo.} Thank you.

1118 Dr. Shannon?

1119 Mr. {Shannon.} Since the public is the hands that  
1120 carries, you know, as you mentioned, carries out the most  
1121 activity, it is the public sector's opportunity to promote  
1122 trust, and that is really one of the distinguishing  
1123 capabilities of our society, and as Jim Lewis has said in our  
1124 venues, it is something that distinguishes us from our  
1125 adversaries may approach things. So promoting trust I think  
1126 is the real opportunity on the government side.

1127 Ms. {Eshoo.} Thank you.

1128 Ms. {Stempfley.} Continue refinement in statute of the  
1129 authorities of the government in a situation--

1130 Ms. {Eshoo.} Excuse me. What?

1131 Ms. {Stempfley.} Continue refinement in statute of  
1132 authorities of organizations such as the Department of  
1133 Homeland Security.

1134 Ms. {Eshoo.} What does that mean?

1135 Ms. {Stempfley.} Excuse me?

1136 Ms. {Eshoo.} What does it mean?

1137 Ms. {Stempfley.} So what that means, ma'am, is what you  
1138 find in the Department is that our authorities are spread  
1139 across multiple statutes and multiple directives, and it is a  
1140 bit of patchwork landscape for us and provides great--

1141 Ms. {Eshoo.} Well, that is the story of DHS.

1142 Ms. {Stempfley.} Yes, ma'am. So if we refine that  
1143 relative to statute, that will put some clarity in terms of  
1144 this and enable stronger information sharing and information  
1145 sharing in action.

1146 Ms. {Eshoo.} Let me ask you something about this--it  
1147 sounds to me like a mini NSA with the center. Do you deal  
1148 with things after the fact and then you can advise federal  
1149 agencies about how a cyber threat has affected them or do you  
1150 defend the workings of agencies so that they don't experience

1151 it? I am not so sure what this group does. We would like to  
1152 come out and see it. Can you answer that for us? I am  
1153 trying to picture it and what you do.

1154 Ms. {Stempfley.} I certainly can, ma'am. We do--we  
1155 provide prevention information and standards for federal  
1156 executive civilian branches to follow that are about raising  
1157 the security of their branch so items they must do in order  
1158 to be--in order to meet the standard, and then we provide  
1159 response actions when something goes wrong as well as  
1160 detection and prevention activities at the boundary.

1161 Ms. {Eshoo.} Well, I am over my time, and I thank all  
1162 of you for not only the work you do but making that come  
1163 alive here in your testimony. Thank you.

1164 Thank you, Mr. Chairman.

1165 Mr. {Walden.} Thank you.

1166 We will now turn to Mr. Terry, the vice chair of the  
1167 subcommittee, for questions.

1168 Mr. {Terry.} Thank you, Mr. Chairman, and I want to  
1169 follow up on both of the sets of questions.

1170 Admiral Barnett, I want to commend you for the job in  
1171 CSRIC, and could you just briefly go over the main  
1172 principles, the five main principles that are outlined by  
1173 CSRIC?

1174 Admiral {Barnett.} There are actually major things, and

1175 I am very pleased to have with me Jeff Goldthorpe, who is our  
1176 Associate Bureau Chief for Cybersecurity, who really led and  
1177 put together this incredible team. So the first one was the  
1178 anti-bot code of conduct for ISPs. All of these address  
1179 ISPs. They are all voluntary industry based. And basically  
1180 the five tenets under the anti-bot thing is education of the  
1181 public so they understand what the problems are, and that  
1182 obviously goes to prevention; detection when they are  
1183 infected; providing notice to them that their computer is  
1184 infected because most of the time they don't realize that  
1185 their computer is infected, and then giving them some tools  
1186 or some resources in order to get their computer cleaned and  
1187 in collaboration to make sure that that information is spread  
1188 across other ISPs so we're refining all this together.

1189         And with regard to DNSSEC, it is encouragement to move  
1190 forward on implementation so to make all DNSSEC servers  
1191 DNSSEC aware, and on the Internet route hijacking, which as  
1192 the chairman mentioned is a little bit arcane and hard to  
1193 understand, but the main thing is, is establish a secure,  
1194 authoritative database in which addresses can be registered  
1195 so this would probably be with the American Registry of  
1196 Internet Numbers. And then ISPs can actually check their  
1197 routes against it and it will be authoritative. They will  
1198 know where it is going. We think this will get rid of all of

1199 the misrouting and will do a lot to help us detect malicious  
1200 routing. So those would be the three main things.

1201 Mr. {Terry.} All right. You mentioned a key phrase in  
1202 there, voluntary and industry based. Can you tell us why it  
1203 is important that standards and ways of implementing what you  
1204 stated should be voluntary and industry based?

1205 Admiral {Barnett.} The FCC as a regulator actually has  
1206 a long history of working with industry to come up with best  
1207 practices. As a matter of fact, the FCC's NRIC, a  
1208 predecessor of CSRIC, came up with the first cybersecurity  
1209 best practices back in 2002. So by getting the experts  
1210 together in the same room and coming up with best practices  
1211 with codes like this, we think we can get a lot of things  
1212 done. And it is also important as CSRIC's work continues to  
1213 make sure that we have the metrics to understand, are those  
1214 voluntary measures actually having the effect we want to so  
1215 CSRIC's work actually continues.

1216 Mr. {Terry.} All right. Starting with you, Ms.  
1217 Alexander, do you agree with those principles?

1218 Ms. {Alexander.} Yes. At NTIA we would very much  
1219 support a multi-stakeholder approach to Internet  
1220 policymaking, and it is really important that the breadth of  
1221 stakeholders that are involved in the ecosystem be part of  
1222 these processes.

1223 Mr. {Terry.} How about voluntary and industry does  
1224 their own standards?

1225 Ms. {Alexander.} Yes, sir.

1226 Mr. {Terry.} Mr. Hutchinson, what do you think?

1227 Mr. {Hutchinson.} I agree with the voluntary nature of  
1228 the standards. One thing that we need, though, is better  
1229 experimentation around what constitutes best practices rather  
1230 than just a declaration. We need to be able to conduct  
1231 experiments.

1232 Mr. {Terry.} Good point.

1233 Mr. Shannon, you are the one non-federal government  
1234 employee at this panel.

1235 Mr. {Shannon.} Yes. I actually participated in the  
1236 2002 NRIC discussions, so I understand the value of that  
1237 collaboration. As the admiral mentioned, I agree that  
1238 putting metrics on place to determine if they are being  
1239 effective is appropriate. You know, take the lightest weight  
1240 approach first. If voluntary compliance works, then that is  
1241 excellent, and it would be wonderful to have metrics that  
1242 confirm that.

1243 Mr. {Terry.} Very good.

1244 And Ms. Stempfley?

1245 Ms. {Stempfley.} Thank you, sir. I believe that the  
1246 innovations that industry provides and the best practices

1247 they provide are incredible useful and very vital in our  
1248 success in this environment and bringing them together in a  
1249 voluntary nature is very important. As we go forward with  
1250 the metrics associated with those, their effectiveness and  
1251 their use I think is the place where we need to--

1252 Mr. {Terry.} There is some effort by some Senators and  
1253 members that state that Homeland Security should be the one  
1254 developing with industry the standards for cybersecurity in  
1255 the private sector. Do you agree with that?

1256 Ms. {Stempfley.} I believe that Homeland Security's  
1257 responsibilities are building standards across critical  
1258 infrastructure and working with the sector experts in each  
1259 sector for standards for cybersecurity.

1260 Mr. {Terry.} How would you develop those standards?

1261 Ms. {Stempfley.} We would develop--

1262 Mr. {Terry.} And how would you enforce them? By rule?

1263 Ms. {Stempfley.} I am sorry, sir. I didn't hear you.

1264 Mr. {Terry.} Would that include developing rules then?

1265 Ms. {Stempfley.} I believe that we need to bring  
1266 industry together in order to determine within each sector  
1267 what is important and then identify where we need to put in  
1268 place best practice and rules or other mechanisms for  
1269 assurance of compliance with best practices.

1270 Mr. {Terry.} I would respectfully state that I

1271 disagree, and I think, frankly, putting an agency in charge  
1272 of developing rules, even with collaboration, is dooming that  
1273 industry. Yield back.

1274 Mr. {Walden.} The gentleman yields back his time.

1275 I now recognize the gentlelady from California, Ms.  
1276 Matsui.

1277 Ms. {Matsui.} Thank you, Mr. Chairman.

1278 An integral part of how the government is asking agency  
1279 reform to IT purchasing involves greater use of the cloud.  
1280 As the government's Chief Information Officer has said, last  
1281 year agencies successfully migrated 40 services to the cloud  
1282 and were able to eliminate more than 50 legacy systems in  
1283 order to save taxpayer dollars while expanding capabilities.  
1284 I have a question for Admiral Barnett, Ms. Alexander and Ms.  
1285 Stempfley. Some of the government agencies here today are  
1286 using cloud services. What can you share with us from your  
1287 early experiences with regard to cyber protections and  
1288 threats? Ms. Alexander?

1289 Ms. {Alexander.} I am actually not the Department's  
1290 expert on cloud issues but I would be happy to make sure we  
1291 get you an answer for the record.

1292 Ms. {Matsui.} Admiral Barnett?

1293 Admiral {Barnett.} Thank you, ma'am. So cloud  
1294 services, my former colleague at FCC, Steve VanRoekel, has

1295 highlighted how valuable cloud services can be. It does  
1296 emphasize the need to make sure that the transport between  
1297 the user agency or company and that cloud is secure and  
1298 reliable. It is another thing that we and I think the people  
1299 that you see at this table are considering is what happens  
1300 for continuity of operations, continuity of government, and  
1301 so there is some considerations we need to make sure on that,  
1302 but really it emphasizes some of the very same things that we  
1303 have talked about today is the network reliability and  
1304 security.

1305 Ms. {Matsui.} Okay. Ms. Stempfley?

1306 Ms. {Stempfley.} Cloud presents some really good  
1307 opportunities to get your arms around configuration  
1308 management and architecting opportunities so to get at the  
1309 root cause. It also has some particular threat opportunities  
1310 as well, as Admiral Barnett indicated, and you have to look  
1311 at it in that holistic lens as we move forward, and it is  
1312 certainly a part of the government's program to do so.

1313 Ms. {Matsui.} Okay. But as the private sector moves  
1314 increasingly to the cloud, what challenges do you foresee?

1315 Ms. {Stempfley.} So I think as Admiral Barnett  
1316 indicated, bringing all of the content together into a single  
1317 place presents a route diversity requirement and a continuity  
1318 requirement. Cloud also presents the opportunity to overcome

1319 that within the way the cloud is architected. So it is a  
1320 wonderful capability for us but it is one of those where it  
1321 is both a challenge and an opportunity simultaneously.

1322 Ms. {Matsui.} Okay. Thank you.

1323 Dr. Shannon, it is my understanding that there are a  
1324 number of clearinghouses, area clearinghouses, that are used  
1325 to store information relating to cyber threats. U.S. CERT  
1326 acts as one of these clearinghouses. What is the  
1327 relationship between those silos and industry and government  
1328 sharing? Can any company access your clearinghouse or do  
1329 they need to be a member of some sort?

1330 Mr. {Shannon.} CERT is part of an FFRDC collaboration  
1331 along with NIST to create vulnerability databases, and that  
1332 is a public resource that is widely available. Of course, we  
1333 also participate in government-focused ones, and that is part  
1334 of the policy decisions that need to be made that are part of  
1335 the discussions about how to share that more broadly.

1336 Ms. {Matsui.} Okay. So with multiple clearinghouses,  
1337 does it make sense to have a streamlined process for  
1338 information sharing for any stakeholder who is threatened  
1339 with attack or at risk?

1340 Mr. {Shannon.} Anyone who is under threat or under  
1341 attack needs to know where to turn to, and I think providing  
1342 that clarity is part of what policymakers can help resolve.

1343 There has been times when CERT has served that purpose, U.S.  
1344 CERT has served that purpose, and as Ms. Stempfley indicated,  
1345 there is confusion.

1346 Ms. {Matsui.} Okay. Admiral Barnett, I am pleased to  
1347 hear you already have commitments from major ISPs to  
1348 implement CSRIC recommendations. How do we share that with  
1349 smaller companies with likely much fewer resources have the  
1350 ability and incentives to do the same?

1351 Admiral {Barnett.} It is a great question, ma'am. One  
1352 of the things I think you will see is that these things are  
1353 going to start becoming the industry standard, reviewing a  
1354 lot of flexibility for companies and how they implement them  
1355 and over what time. Hopefully they can do them along with  
1356 their normal business processes working with the American  
1357 Cable Association or maybe the smaller systems to figure out  
1358 what are the best ways, and one of the major things, as I  
1359 mentioned, CSRIC's work continues. The next things that we  
1360 set them on is, what are the barriers to implementation, how  
1361 do we get over those. So these same great experts are going  
1362 to come back together and start working on those very things.

1363 Ms. {Matsui.} So there is a concerted effort to reach  
1364 out to some of the smaller companies?

1365 Admiral {Barnett.} Yes, ma'am.

1366 Ms. {Matsui.} Okay. That is great. Good.

1367           Let me see. Dr. Shannon, in your testimony, you stress  
1368 the importance of secure coding so initiatives such as  
1369 addressing root causes of cyber threats. Is this concept  
1370 applicable to apps that are downloaded to mobile devices that  
1371 connect to the Internet such as smartphones and our tablets?

1372           Mr. {Shannon.} Yes. It is highly applicable. I mean,  
1373 there is two parts of the app's development environment. One  
1374 is the infrastructure and that needs to be coded securely.  
1375 Fortunately for the app developers, there is a more  
1376 constrained environment so it is a possibility for the  
1377 ecosystem owner to help protect the users and to ensure that  
1378 the app developers are developing appropriate apps. But part  
1379 of it is, is that, you know, we will find vulnerabilities  
1380 there and that is how you train, you know, the teenagers that  
1381 are writing the apps to write them correctly. I mean, it is  
1382 a serious challenge but, you know, it is that balance with  
1383 innovation.

1384           Ms. {Matsui.} Sure. Okay. Thank you very much.

1385           Mr. {Walden.} You hire them at Sandia Labs.

1386           We will go now to the gentlelady from California, Ms.  
1387 Bono Mack, for questions.

1388           Mrs. {Bono Mack.} Thank you, Mr. Chairman.

1389           Ms. Stempfley, I can't see you over there, but my first  
1390 question is directed to you. Since Congress created the

1391 Chemical Facility Antiterrorism Standards, or what we call  
1392 CFATS, program in 2007, there have been ongoing problems with  
1393 the way DHS has managed the program. These problems include  
1394 DHS improperly tiering 600 chemical facilities, wasteful  
1395 spending and the inability of DHS to properly train the  
1396 workforce responsible for carrying out the chemical security  
1397 program. Hundreds of millions have been spent on CFATS. We  
1398 find ourselves with a program that has been mismanaged,  
1399 wasted taxpayer dollars, and no assurance that our chemical  
1400 facilities are in fact secure.

1401 Can you tell me with these significant problems in the  
1402 instance of CFATS how you could possibly assert to this  
1403 committee that DHS will not mismanage cybersecurity?

1404 Ms. {Stempfley.} Ma'am, thank you very much for the  
1405 opportunity to address that. The differences between  
1406 chemical facilities and information technology and  
1407 communication are fairly profound in that situation, and so  
1408 as we work as a department of experts brought together and  
1409 engage in these discussions with industry about what are the  
1410 basic standards that are necessary, we envision building  
1411 those basic standards in that scenario and then learning  
1412 lessons across the Department from areas where we have worked  
1413 through issues. We want to ensure that we don't make the  
1414 same mistakes a second time.

1415 Mrs. {Bono Mack.} With all due respect, I didn't really  
1416 hear an answer in your answer, but I would say to you that  
1417 perhaps there are differences between chemical facilities and  
1418 cybersecurity yet I think from the American people's point of  
1419 view, it is the bureaucracy, and I think you have rattled off  
1420 quite a list of acronyms but I don't know that my  
1421 constituents would feel safer by the list of acronyms that  
1422 you have used. In fact, to me, did I mishear you? The  
1423 example of the EDA's website or network being down for weeks  
1424 when you were asked a question by the chairman, you know,  
1425 what do you and you are responsible for prevention and  
1426 mitigation. Is that not an example, though, of failure of  
1427 all of these bureaucracies to in fact work together well?

1428 Ms. {Stempfley.} The example presented by the chairman,  
1429 ma'am, with Commerce is an example where we in the Department  
1430 and the Department of Commerce have joint action that must be  
1431 taken. So in that scenario, the Department of Commerce has  
1432 the responsibility for the management and security of their  
1433 systems in building them and in operating them following the  
1434 standards set by the Department of Homeland Security.

1435 Mrs. {Bono Mack.} Thank you.

1436 To Admiral Barnett, you know, I agree that the federal  
1437 government should be involved in our country's cybersecurity  
1438 efforts, absolutely, but they should be enhancing cooperation

1439 and they should be the facilitator, not a regulator. Can you  
1440 elaborate a little bit on your thoughts on the value of a  
1441 cooperative relationship with the private sector versus a  
1442 regulatory one?

1443       Admiral {Barnett.} Yes, ma'am. So certainly the CSRIC  
1444 actions last week are an example of that, but there are many,  
1445 many others. CSRIC also addresses cooperation in the  
1446 telecommunications industry on next-generation 911, on  
1447 emergency learning, and as Dr. Shannon mentioned, we have  
1448 done this for years and years. I think it is helpful when  
1449 you have the regulator who is the expert in the United States  
1450 to be involved with this. They will sit down with industry,  
1451 just like the experts that I mentioned that I brought with me  
1452 today. We have experts in other areas like the ones I have  
1453 mentioned in next-generation 911, to be able to sit down with  
1454 industry to pull them together, and quite frankly, that is  
1455 one of the reasons that we were able to pull together these  
1456 experts to come up with voluntary industry-based solutions.

1457       Mrs. {Bono Mack.} Thank you. I think my biggest  
1458 concern is recognizing how quickly the cyber world knows and  
1459 the bad guys are by nature one step ahead of the good guys,  
1460 so the question really is, with all of the regulatory hurdles  
1461 potentially, how do we really keep pace with the threat?

1462       Admiral {Barnett.} Yes, ma'am. So recognizing that the

1463 large majority of telecommunications cybersecurity are in  
1464 private hands, there is a couple things to that. They are  
1465 the first lien of defense. Our actions, and I think what you  
1466 have heard mostly from these panelists, is to enhance those  
1467 but we also have to recognize something else. It is not  
1468 working. We wouldn't be here concerned about this if that  
1469 was enough, and so as Dr. Shannon mentioned, we have to have  
1470 metrics to make sure that the voluntary methods that we are  
1471 employing work, and then beyond that to look at whatever  
1472 else. Hopefully there would be other things that we could  
1473 do, so information sharing is one thing. There may be other  
1474 best practices that we can do. But the thing that is an  
1475 absolutely prerequisite on this is, we have to make sure that  
1476 they are effective because we cannot go on any longer the way  
1477 we are now.

1478 Mrs. {Bono Mack.} Thank you. My last question, and  
1479 then I am out of time. To any of you, are government  
1480 agencies able to effectively combat cyber agitators that we  
1481 are very well aware of right now like Anonymous and WILSEC  
1482 and what are we doing to stop their attacks. To anybody I  
1483 will pose that question and then I am out of time.

1484 Ms. {Stempfley.} Government departments and agencies  
1485 every day are working to defend against threats as you  
1486 indicated both in terms of Anonymous and WILSEC, and in the

1487 instance where they have been unsuccessful, we work in  
1488 partnership to help them overcome the impacts of those  
1489 attacks in that situation through a layered defense strategy  
1490 which includes things like the Einstein program and things  
1491 like the establishment of standards through the federal  
1492 network security programs.

1493 Mr. {Shannon.} I would say just briefly, I would  
1494 encourage you to talk to the law enforcement community. I  
1495 think they have been doing a very effective job given some of  
1496 the recent arrests in that area.

1497 Mrs. {Bono Mack.} All right. Thank you, Mr. Chairman,  
1498 for the time and I yield back.

1499 Mr. {Walden.} The gentlelady yields back, and Admiral  
1500 Barnett, we agree with you on the accountability and matrix  
1501 and all that.

1502 Mr. Dingell for 5 minutes.

1503 Mr. {Dingell.} Thank you, Mr. Chairman. I hope you are  
1504 not still smarting from yesterday's handling of that  
1505 legislation.

1506 Good morning. This first question will be to all  
1507 witnesses yes or no. Ladies and gentlemen, industry  
1508 witnesses told this subcommittee on March 7, 2012, that the  
1509 federal government would facilitate better interindustry and  
1510 public-private information sharing. Do you agree with that

1511 opinion? Yes or no, starting with Ms. Alexander.

1512 Ms. {Alexander.} Yes.

1513 Mr. {Dingell.} Admiral?

1514 Admiral {Barnett.} Yes, information sharing can be a  
1515 government role.

1516 Mr. {Dingell.} Just yes or no, because I am running out  
1517 of time.

1518 Mr. {Hutchinson.} Yes.

1519 Mr. {Shannon.} Yes.

1520 Mr. {Dingell.} Ma'am?

1521 Ms. {Stempfley.} Yes.

1522 Mr. {Dingell.} Good. Again, to all witnesses, again,  
1523 yes or no. Senator Lieberman's cybersecurity bill, S. 2105,  
1524 requires the Secretary of Homeland Security to promulgate  
1525 risk-based cybersecurity performance requirements for owners  
1526 of critical infrastructure. Do you believe the promulgation  
1527 of such requirements is wise? Yes or no.

1528 Ms. {Alexander.} Yes.

1529 Mr. {Dingell.} Admiral, they don't have a nod button.  
1530 You have to say yes or no.

1531 Admiral {Barnett.} Yes.

1532 Mr. {Dingell.} All right. Next witness.

1533 Mr. {Hutchinson.} Yes.

1534 Mr. {Shannon.} No comment.

1535 Ms. {Stempfley.} Yes.

1536 Mr. {Dingell.} Thank you. Now, this is for all  
1537 witnesses. Similarly, do you believe promulgation of such  
1538 performance requirements would stifle innovation and harm  
1539 industry's ability to protect consumers from cyber threats?  
1540 Yes or no. Ms. Alexander?

1541 Ms. {Alexander.} No.

1542 Mr. {Dingell.} Admiral?

1543 Admiral {Barnett.} No.

1544 Mr. {Dingell.} Next witness.

1545 Mr. {Hutchinson.} Yes.

1546 Mr. {Dingell.} Next witness.

1547 Mr. {Shannon.} It is a risk.

1548 Mr. {Dingell.} Next witness.

1549 Ms. {Stempfley.} No.

1550 Mr. {Dingell.} All right. Now, Admiral Barnett, you  
1551 mentioned in your testimony the Communications Security,  
1552 Reliability and Interoperability Council--that is CSRIC--  
1553 recommendations about preventing domain name spoofing, route  
1554 hijacking and botnet attacks. These recommendations are  
1555 voluntary, are they not?

1556 Admiral {Barnett.} Yes, sir.

1557 Mr. {Dingell.} Now, again, Admiral, how many Internet  
1558 service providers--ISPs--have adopted CSRIC's

1559 recommendations?

1560 Admiral {Barnett.} There are nine Internet service  
1561 providers that have pledged to implement those  
1562 recommendations.

1563 Mr. {Dingell.} Out of how many?

1564 Admiral {Barnett.} Well, there are literally thousands,  
1565 I guess, when you start talking about the small cable  
1566 operators, and we are working with the various associations--

1567 Mr. {Dingell.} So what you are telling me is, you have  
1568 a penetration of nine out of thousands?

1569 Admiral {Barnett.} Well, we have a penetration that  
1570 will cover 80 percent of American Internet users right from  
1571 the beginning and we will continue to go towards 100 percent.

1572 Mr. {Dingell.} Of course, if they can shut down your  
1573 banking industry, they can shut down your electrical utility  
1574 industry, your handling of your net, they could shut down the  
1575 natural gas pipeline system in this country, refineries, auto  
1576 companies, God knows what else they can shut down with that  
1577 kind of opportunity available.

1578 Admiral {Barnett.} That is why we are going to continue  
1579 to work for 100 percent.

1580 Mr. {Dingell.} When will you hit 100 percent? Do you  
1581 have any idea?

1582 Admiral {Barnett.} We don't at this particular point

1583 but I felt pretty good about getting 80 percent commitment  
1584 from the beginning, and we are going to continue work on the  
1585 barriers to implementation so that we can get even the  
1586 smaller Internet service providers as soon as possible.

1587 Mr. {Dingell.} All right. Now, to all witnesses,  
1588 similarly, can and should CSRIC's recommendations be adopted  
1589 by the FCC or other federal agencies and thereby be made  
1590 mandatory? Please answer yes or no, but I would very much  
1591 appreciate a written submission explaining your comment,  
1592 starting with you, Ms. Alexander.

1593 Ms. {Alexander.} No.

1594 Mr. {Dingell.} Admiral?

1595 Admiral {Barnett.} No, sir.

1596 Mr. {Dingell.} Next witness.

1597 Mr. {Hutchinson.} No.

1598 Mr. {Shannon.} Only when there is supporting data.

1599 Mr. {Dingell.} Next witness.

1600 Ms. {Stempfley.} No, sir.

1601 Mr. {Dingell.} Thank you. And please submit that. I  
1602 am sorry to do that to you but the time here is rather  
1603 limited.

1604 Ms. Alexander, your testimony focused largely on domain  
1605 name security extensions. As you know, Internet Corporation  
1606 for Assigned Names and Numbers, ICANN, has signaled its

1607 intention to increase by many fold the number of generic top-  
1608 level domain names. Is NTIA concerned that such expansion  
1609 may complicate efforts to deploy DNSSEC as well as compromise  
1610 DNSSEC's future effectiveness? Yes or no.

1611 Ms. {Alexander.} No, sir, it is a requirement.

1612 Mr. {Dingell.} Would you submit an appropriate further  
1613 response on that matter?

1614 Ms. {Alexander.} Absolutely.

1615 Mr. {Dingell.} Now, other witnesses, do any of you,  
1616 starting with you, Admiral, care to comment on Ms.  
1617 Alexander's comments?

1618 Admiral {Barnett.} No, sir.

1619 Mr. {Dingell.} Next witness.

1620 Mr. {Hutchinson.} No comment.

1621 Mr. {Dingell.} Next witness.

1622 Mr. {Shannon.} Any technology that hasn't been deployed  
1623 for decades may potentially have vulnerabilities, and that is  
1624 always a fundamental challenge in the age of the Internet.  
1625 There are unforeseen uses decades down the road. Leading  
1626 academics have contributed to DNSSEC. It is one of our best  
1627 efforts to try and tackle these issues, so I am confident  
1628 that it will stand the test of time.

1629 Mr. {Dingell.} Ms. Stempfley?

1630 Ms. {Stempfley.} No comment.

1631 Mr. {Dingell.} Thank you.

1632 Thank you, Mr. Chairman, for your courtesy.

1633 Mr. {Walden.} Thank you.

1634 We will now go to Ms. Blackburn for 5 minutes for  
1635 questions.

1636 Mrs. {Blackburn.} Thank you, Mr. Chairman, and I want  
1637 to thank all of you for your time and for being here.

1638 Mr. Hutchinson, I want to come to you first and ask you  
1639 about the program that you all have that you liken to a  
1640 medical residency in cybersecurity. So what I would like to  
1641 know is how that is structured, if you could give us a little  
1642 bit more detail. Is it public-private partnership? And the  
1643 reason I ask this is because in the area that I represent in  
1644 Tennessee, there around Nashville, we have so many  
1645 individuals that started working on the entertainment  
1646 industry platforms and they have moved to defense informatics  
1647 or over to health care informatics and then some of them are  
1648 in financial service informatics, and we see so much sharing  
1649 on the skills that are there to keep the backbone of the  
1650 Internet safe, if you will, and I think it is fascinating  
1651 that you all have done something, but as we talk about having  
1652 a trained workforce who is able to handle this, it sounds  
1653 like a good idea and I would love a little detail if you are  
1654 able to share that.

1655 Mr. {Hutchinson.} Yes. Thank you for that question.  
1656 What we realized is that technology is nowhere near ready to  
1657 protect our networks, that it really requires people and it  
1658 requires creative people who can adapt to lots of technology  
1659 and tools. When we built this program, we focused on  
1660 bringing the participants together in a common environment,  
1661 to carefully pair those individuals and team them with  
1662 mentors, and to create--

1663 Mrs. {Blackburn.} Let me stop you right there. How do  
1664 you select individuals for this program? How do you pick  
1665 them out and select them?

1666 Mr. {Hutchinson.} Okay. So in the early days, we  
1667 selected them through an application and résumé and interview  
1668 process. Today, there is a lot of referrals, so we get  
1669 referrals from people who understand this program, and so we  
1670 place them in this environment. They work together on teams.  
1671 They work on actual national security problems. They learn  
1672 security through that experience. They learn all the  
1673 balances and the gives and takes and what makes cybersecurity  
1674 particularly difficult, and as they build these projects out  
1675 and make these tradeoffs, they just gain the type of instinct  
1676 that a medical student must also gain in a residency program.

1677 Mrs. {Blackburn.} Okay. That sounds great. Now, any  
1678 of the graduates of your program, if you will, and I use that

1679 just as a term to kind of look at those that have come  
1680 through, how many have come through the program?

1681 Mr. {Hutchinson.} So I can provide an exact number for  
1682 the record but it is about 500.

1683 Mrs. {Blackburn.} Okay. That sounds wonderful. Have  
1684 any of them been helpful going forward in identifying risk or  
1685 threats to the system or maybe writing programs that help to  
1686 foil any of the threats? What kind of participation and  
1687 results are you seeing?

1688 Mr. {Hutchinson.} So the people who have been through  
1689 this program are distributed to industry, they are in  
1690 government service, they work for national labs and other  
1691 FFRDCs, and there are many cases where they have developed  
1692 tools that were able to identify a particular breach of a  
1693 network or to develop algorithms that can provide things like  
1694 directions toward attribution and criminal investigation,  
1695 digital forensics capability. There is a long list of  
1696 achievements.

1697 Mrs. {Blackburn.} So you are seeing solid results?

1698 Mr. {Hutchinson.} Solid results from these individuals.

1699 Mrs. {Blackburn.} Okay. That sounds great.

1700 This is something I would like to hear from each of you,  
1701 and I only have 1 minute left. As I mentioned earlier, we  
1702 are working on cybersecurity legislation, and the question

1703 that always come up is, how narrow do you make it or how  
1704 broad. And I have appreciated hearing your testimonies  
1705 today. So how narrowly or broadly should federal legislation  
1706 define what can or cannot be shared between governments and  
1707 private entities and should there be specific requirements on  
1708 PII about innocent consumers being taken out of data packets  
1709 before it can be shared with any other government agencies?

1710 Mr. {Shannon.} I encourage you to consider legislation  
1711 that is broad in the sense of supporting people who need to  
1712 do the right thing in response to incidents. In terms of  
1713 more prescriptive approaches, I encourage you to use data-  
1714 driven, you know, pilots essentially to verify that a policy  
1715 that is being considered that may be prescriptive is actually  
1716 going to be effective.

1717 Mrs. {Blackburn.} Okay.

1718 Ms. {Stempfley.} I would like the opportunity to come  
1719 back to you via technical assistance or others and describe  
1720 the processes we use in the Department today for how to  
1721 protect privacy and other considerations where what we are  
1722 mostly focused on are indicators, the specific technical  
1723 pieces of information that are useful. While it is not  
1724 possible to always avoid in that indicator selection of some  
1725 things that may be of concern, we have strong protection  
1726 measures in place to ensure as we are working to get to the

1727 indicators the malicious code, so I would like to follow up.

1728           Mrs. {Blackburn.} Thank you. I appreciate that. I  
1729 yield back.

1730           Mr. {Walden.} I thank the gentlelady and now I turn to  
1731 Mr. Stearns for final questions.

1732           Mr. {Stearns.} Thank you, Mr. Chairman. I think maybe  
1733 you heard my opening statement talking about Shawn Henry, the  
1734 FBI's top cyber cop, and so I was going to ask each of you  
1735 starting with you, Ms. Alexander, Mr. Henry told the Wall  
1736 Street Journal that we are not winning the cybersecurity  
1737 battle. He went on to say ``We have been playing defense for  
1738 a long time, and you can only build a fence so high, and what  
1739 we found is that the difference that the offense outpaces the  
1740 defense and the offense is better than the defense. Do you  
1741 agree or disagree with the assessment of Shawn Henry?

1742           Ms. {Alexander.} Thank you very much, Congressman. I  
1743 am not familiar with the article or what he said but I would  
1744 say he just points to the reason why we are here today and  
1745 why we are all working so closely across the federal  
1746 government to be vigilant dealing with these issues.

1747           Mr. {Stearns.} Admiral?

1748           Admiral {Barnett.} Yes, sir, I would agree with him.  
1749 We cannot sustain the way it is going right now. We have too  
1750 much of our economy that is now invested in ones and zeros.

1751 There are so many other things, verticals, critical  
1752 infrastructures, that depend on our communication  
1753 infrastructure to impact it. So we have to take action, and  
1754 so I think what you have heard here today is a call for that.  
1755 And in answer to your response, we appreciate this hearing to  
1756 focus on it.

1757 Mr. {Stearns.} Mr. Hutchinson?

1758 Mr. {Hutchinson.} Attackers do have an easier job than  
1759 a defender has, and that is problematic, and it is resource-  
1760 depleting. I completely agree with the assessment that the  
1761 defenders are on the wrong side economically. I mean, it is  
1762 very easy for an attacker to attack a system and cause a lot  
1763 of money to be spent in defending that system. But the  
1764 solution is to accept that our networks will never be free of  
1765 compromise and to find ways that we can operate in the face  
1766 of compromise, and that is an open research challenge. There  
1767 is certain progress in that direction and I would encourage  
1768 additional support for those forms of research objectives.

1769 Mr. {Stearns.} Dr. Shannon?

1770 Mr. {Shannon.} It is a dramatic article. I have not  
1771 read it. It is certainly the sort of articles that we have  
1772 seen for many decades in the area of cybersecurity. They  
1773 just tend to get more press these days.

1774 You know, I would encourage you to remember that it is

1775 about root causes versus innovation. You know, we all  
1776 received email this morning, the sky isn't falling. There  
1777 are serious, serious challenges but it is easy to get a  
1778 little carried away, in my view.

1779 Mr. {Stearns.} So would you agree with him or not?

1780 Mr. {Shannon.} I don't think it is just going to be so  
1781 dramatic.

1782 Mr. {Stearns.} Okay.

1783 Mr. {Shannon.} That is my personal opinion.

1784 Mr. {Stearns.} I appreciate your honesty here.

1785 Mr. {Shannon.} After being with colleagues who were  
1786 dramatic, you know, 20 years ago about these issues.

1787 Mr. {Stearns.} Okay. Ms. Stempfley?

1788 Ms. {Stempfley.} Thank you, sir, and thank you for the  
1789 opportunity with this hearing because I think the thematics  
1790 of that article are certainly what we are talking about  
1791 today, and as I said, there is no single solution in this  
1792 situation, and so if the premise of the article is that we  
1793 need to make changes in order to increase awareness and  
1794 importance of the cybersecurity challenges, then I would  
1795 agree with that.

1796 Mr. {Stearns.} Okay. Admiral Barnett, I think you told  
1797 Ms. Eshoo earlier that we need to focus on supply chain  
1798 vulnerabilities. I had a hearing as chairman of the

1799 Oversight and Investigations Subcommittee yesterday just on  
1800 that with the Department of Energy, and frankly, they are  
1801 doing catch-up. CBO had a report that came out mentioning  
1802 that the Department of Defense and the DOE admit that they  
1803 just started looking at ways to look at cybersecurity in the  
1804 supply chains. So I just wonder if you had anything you  
1805 would like to elaborate on on the supply chain  
1806 vulnerabilities.

1807       Admiral {Barnett.} Well, at the FCC we have been  
1808 looking at this for the 2 years that I have been there, and I  
1809 know we have been working with other governmental partners on  
1810 this. One of the things that is apparent as we look across  
1811 the authorities for whatever else you can say about it is the  
1812 authorities that we have right now were not designed to  
1813 address the supply chain challenges we have right now, so  
1814 additional work needs to continue. There are a couple of  
1815 approaches that I hear going on. One is a kind of a  
1816 transactional approach. One I think I am intending to favor  
1817 better right now is a supply chain risk management where it  
1818 is a tiered approach, and the most critical elements of our  
1819 communications network are provided the most protection.  
1820 That allows a little bit more flexibility as you go down to  
1821 the other tiers. There are a lot of tools that are available  
1822 to us that may include various supply chain standards. The

1823 government needs to work together on this to pull together  
1824 and we can't start soon enough.

1825 Mr. {Stearns.} Mr. Hutchinson, according to your  
1826 president and director, Paul Himmert, Sandia National  
1827 Laboratories have been attacked up to 30,000 times per hour.  
1828 Do some of these attacks get through your safety net? Does  
1829 Sandia National Laboratories currently have supply chain  
1830 checks in place with equipment that you buy?

1831 Mr. {Hutchinson.} Okay. The attacks that lab Director  
1832 Himmert is referring to are not supply chain attacks per se  
1833 but just operational attacks against our cyber networks and  
1834 they are measured that way because we have successfully  
1835 identified that as an attack and stopped it before it  
1836 affected our systems. And that said, we have instances where  
1837 we detect compromises that occurred on our systems and we  
1838 investigate and address those as we discover them. And yes,  
1839 we do have very careful supply chain processes that we follow  
1840 because our prime mission of building weapons has been a  
1841 victim or has been a target, not a victim, a target of supply  
1842 chain attacks for many years. So we have developed our end-  
1843 sharing and science capabilities to address those issues.

1844 Mr. {Stearns.} Thank you, Mr. Chairman.

1845 Mr. {Walden.} I thank the gentleman for his questions.

1846 Seeing no other members to ask questions, thank you very

1847 much for your testimony, for your answers to the questions,  
1848 and the good work you are doing to make America safer and  
1849 more secure. We appreciate it in this role and in other  
1850 roles that you have had. And I thank the subcommittee  
1851 members for their participation. We will continue on this  
1852 topic, although I don't see future hearings at the moment  
1853 planned, but we will be in contact with you, and I know some  
1854 of our colleagues have questions for you to follow up on, so  
1855 we appreciate your written responses to those and any other  
1856 suggestions you have for us. We want to get this right, and  
1857 there is too much at stake not to.

1858           So we appreciate your help and I appreciate the  
1859 participation of the committee, and with that, we stand  
1860 adjourned.

1861           [Whereupon, at 11:38 a.m., the Subcommittee was  
1862 adjourned.]