

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

1 {York Stenographic Services, Inc.}  
2 RPTS MEYERS  
3 HIF059.020

4 ``CRITICAL INFRASTRUCTURE CYBERSECURITY: ASSESSMENTS OF  
5 SMART GRID SECURITY  
6 TUESDAY, FEBRUARY 28, 2012  
7 House of Representatives,  
8 Subcommittee on Oversight and Investigations  
9 Committee on Energy and Commerce  
10 Washington, D.C.

11 The Subcommittee met, pursuant to call, at 10:19 a.m.,  
12 in Room 2322 of the Rayburn House Office Building, Hon. Cliff  
13 Stearns [Chairman of the Subcommittee] presiding.

14 Members present: Representatives Stearns, Terry,  
15 Burgess, Blackburn, Myrick, Gingrey, DeGette, and Waxman (ex  
16 officio).

17 Staff present: Carl Anderson, Counsel, Oversight; Todd  
18 Harrison, Chief Counsel, Oversight and Investigations; Katie

19 Novaria, Legislative Clerk; Andrew Powaleny, Deputy Press  
20 Secretary; Alvin Banks, Democratic Investigator; Brian Cohen,  
21 Democratic Investigations Staff Director and Senior Policy  
22 Advisor; and Kiran Gopal, Democratic Counsel.

|  
23           Mr. {Stearns.} Good morning, everybody. I call the  
24 Subcommittee's second hearing on cybersecurity and critical  
25 infrastructure protection to order.

26           My colleagues, America's infrastructure systems have  
27 become more automated and more reliant on information systems  
28 and computer networks to operate. While our systems are more  
29 efficient, they also open the door to cyber threats and  
30 cyber-attacks. Today, the Subcommittee focuses on that part  
31 of the critical infrastructure known as smart grid, which  
32 refers to the information technology systems increasingly  
33 incorporated into the Nation's electricity networks.

34           Smart grid technologies are designed to lower operation  
35 costs, reduce maintenance costs, and expand the flexibility  
36 of operational control relative to the current grid system.  
37 Their operational efficiency and improved asset use is driven  
38 by advanced communication and information technologies.

39           I believe that we must update our electric grid with  
40 better technology integration, which is why I spearheaded the  
41 effort to secure funding for Energy Smart Florida, the  
42 largest smart grid demonstration project in the country.  
43 This initiative will invest hundreds of millions of dollars  
44 in smart grid technology and renewable energy in Florida and  
45 throughout the entire county. Energy Smart Florida will

46 revolutionize how people use energy in their homes and enable  
47 them to make smarter choices about energy consumption and  
48 better control their carbon emissions. In addition, the  
49 widespread deployment of smart meters will provide Floridians  
50 with more reliable electrical service through an intelligent  
51 network that will be able to detect potential problems and  
52 automatically reconfigure the grid to minimize or eliminate  
53 outages.

54         But ask any expert in the national security field and  
55 see what keeps them up at night. They would probably tell  
56 you, as they tell me, that it is the increased possibility of  
57 a devastating cyber-attack. This threat is real and is why  
58 it is virtually important--vitaly important for us to do  
59 what we can to protect our critical infrastructure from these  
60 threats. We have seen in the past decade what impact both  
61 man-made and natural disasters have on our Nation's utility  
62 systems. Imagine the impact of a cyber-attack to the  
63 electrical grid. How many days could hospitals operate with  
64 onsite electric generation? How would metro rail systems  
65 operate, if at all? How would we recharge our smart phones  
66 or access the internet? The goal of the smart grid is to  
67 improve efficiency, reliability and interoperability. An  
68 equal goal, however, must be to improve upon the security  
69 controls and to minimize the impact from a man-made or

70 natural disaster to ensure reliability and avoid such  
71 possibilities.

72         Now, a recent report completed by the Pike Research  
73 company estimated that utilities' initiatives to secure their  
74 infrastructure will drive increasing investments to involve  
75 cybersecurity systems and total roughly \$14 billion from now  
76 through the year 2018. While the Department of Energy has  
77 emphasized investment in technologies such as smart meters,  
78 among other technologies, we want to ensure that where there  
79 is investment, there is not a security--cybersecurity gap.  
80 We want to emphasize that there is also investment in  
81 securing control system segments including transmission  
82 upgrades, substation automation, and distribution automation  
83 systems.

84         Protecting critical infrastructure is a complicated  
85 issue. We are talking about facilities and frameworks owned  
86 by private companies, and by federal, State, and local  
87 governments. They are interconnected. Electricity powers  
88 water systems that cool nuclear reactors, for example. They  
89 are vulnerable to threats from a number of different sources,  
90 including nation-states, criminals, and hackers.

91         The issues surrounding critical infrastructure  
92 protection and security are complex. To help analyze these  
93 complexities, I am pleased to be joined by our panel of

94 experts in the field. Today, we will hear testimony from two  
95 witnesses at GAO: Mr. Gregory Wilshusen, Director of  
96 Information Security Systems, and Mr. David Trimble, Director  
97 of Natural Resources and the Environment. I look forward to  
98 their testimony, and getting a better understanding of their  
99 extensive work examining cybersecurity implications of the  
100 smart grid. I also would like to welcome Mr. Richard  
101 Campbell, of the Congressional Research Service, who has  
102 examined this very subject and we look forward to his  
103 contributions today.

104 My colleagues, as I mentioned previously, this is the  
105 Subcommittee's second hearing in this Congress on critical  
106 infrastructure protection and cybersecurity. The purpose of  
107 this hearing, in particular, is to get an overview of smart  
108 grid cybersecurity, and how it is working and what can be  
109 done better. It is my intention to call the Department of  
110 Energy and possibly other stakeholders to a future hearing  
111 for further consideration of smart grid security.

112 I have enjoyed working with the Ranking Member, Ms.  
113 DeGette and the Minority in these matters and look forward to  
114 working with them on overseeing cybersecurity issues again.  
115 So I look forward to this hearing, the perspectives of our  
116 expert witnesses about the safety of this vital part of  
117 critical infrastructure, and whether we are taking the right

118 steps to protect them from cybersecurity risks and threats.

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

120 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
121           Mr. {Stearns.} And with that, I recognize the Ranking  
122 Member, Ms. DeGette.

123           Ms. {DeGette.} Thank you very much, Mr. Chairman, for  
124 holding this hearing on smart grid cybersecurity.

125           Last year in July, representatives of the Department of  
126 Homeland Security came before this Subcommittee to discuss  
127 their efforts to protect and deploy federal resources and to  
128 coordinate with the private sector to prevent and respond to  
129 cyber attacks. This hearing, as you mentioned, is an  
130 important follow-up to that hearing.

131           Protecting our critical infrastructure from cyber  
132 attacks is, of course, of vital importance. As our electric  
133 grid evolves, we become more and more dependent on so-called  
134 smart technologies to control, connect, and maintain this  
135 interconnected system. This is a good thing. It will make  
136 the grid more efficient and more reliable. For example,  
137 consumers will soon be able to track the price of electricity  
138 minute by minute and adjust electricity use accordingly,  
139 waiting, for example, until prices are right to do the  
140 laundry or start the dishwasher.

141           However, these investments also expose us to new  
142 threats. These new technologies can be easy prey for hackers  
143 or terrorists who seek to bring down unprotected networks.

144 As the smart grid becomes more interoperable, these attacks  
145 could have debilitating effects nationwide, as you mentioned,  
146 Mr. Chairman. In 2007, DHS ran a test known as Aurora, which  
147 showcases just how dangerous grid vulnerabilities can be.  
148 They used a dial-up modem to rewrite computer code and  
149 remotely detonate an industry-controlled system generator.  
150 That is why I am pleased we are having this hearing today.  
151 We as a Congress must do everything in our power to ensure  
152 that the grid remains safe and secure.

153 The testimony we hear today will help us understand our  
154 successes and identify flaws in the current approach so that  
155 we can understand what else can be done to protect the smart  
156 grid. This hearing will also help us understand if Congress  
157 needs to provide more resources or more legislative authority  
158 for key cybersecurity agencies.

159 The Administration has made cybersecurity a priority,  
160 launching a comprehensive national cybersecurity initiative  
161 to protect the digital infrastructure. The President's 2013  
162 budget includes \$769 million to support the National  
163 Cybersecurity Division within the Department of Homeland  
164 Security. These funds are targeted at improving monitoring  
165 on federal networks to respond to cyber threats, and  
166 supporting cyber attack responses for critical infrastructure  
167 owners and operators, and for State and local authorities.

168 I commend this targeted focus on cybersecurity, but I am  
169 hoping that today our witnesses will help us learn more about  
170 any gaps in security that may still exist.

171 Mr. Chairman, as I said, I appreciate that you are  
172 holding this hearing, and I am encouraged that you have  
173 announced that we are going to keep looking into other areas  
174 where we can work together in a bipartisan fashion. For  
175 example, we will hear from witnesses today the issue of  
176 cybersecurity goes well beyond the protection of the critical  
177 infrastructure. Consumers entrust important personal  
178 information on their banks--to their banks, their internet  
179 service providers, their credit card companies, and the  
180 retailers from whom they purchase items from online. These  
181 companies should ensure that they are protecting this  
182 information and Congress needs to be doing its oversight job  
183 to make sure that this is the case.

184 Every day we hear stories about e-mail accounts being  
185 hacked, credit card information being hijacked, and Social  
186 Security numbers or other important personal information  
187 being stolen by cyber criminals. It has even happened to  
188 some of us who sit on this panel. The loss of this  
189 information can be costly and personally damaging. In  
190 September of last year, the internet security company,  
191 Symantec, issued the Norton Cyber Crime Report and calculated

192 that cyber crimes cost companies and consumers \$114 billion  
193 annually. That same report found that more than 2/3 of  
194 adults online had been victims of a cyber crime.

195 As our use of internet services becomes more and more  
196 integrated, using the same internet services for e-mail,  
197 social networking, photo sharing, bill paying, and browsing  
198 and search, we have to be more vigilant in ensuring the  
199 protection of our personal information. Sites like Google,  
200 Yahoo, and Facebook will be targets for hackers, and if  
201 successful, these cyber attacks will have a major impact on  
202 the American public.

203 For that reason, Mr. Chairman, in addition to  
204 investigating how the government can improve critical  
205 infrastructure cybersecurity, I think this Subcommittee  
206 should also look closely at what the private sector is doing  
207 to prevent cyber attacks and keep consumers' personal  
208 information safe.

209 I look forward to working with you on all of these  
210 issues, Mr. Chairman, and with that, I will yield back.

211 [The prepared statement of Ms. DeGette follows:]

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

|  
213           Mr. {Stearns.} Thank the gentlelady and recognize the  
214 gentleman from Nebraska, Mr. Terry, for 2 minutes.

215           Mr. {Terry.} Thank you, Mr. Chairman, for holding this  
216 important hearing. Of course, one of the cornerstone  
217 responsibilities of this Committee is finding--determining  
218 reliability of our electricity delivery system. In today's  
219 world, that means when we are protecting the grid, it means  
220 we have to look into the cyber attacks.

221           Let me just give you one quick story from University of  
222 Nebraska at Omaha, PKI Institute of Information Assurance.  
223 They set up as a class project in their master's program an  
224 electric company fake website, and then tracked who would  
225 attack it. Within about 48 hours, there was probably about  
226 50 hack attempts, most of them coming from a certain region  
227 in China, but all over the world. This just shows how  
228 vulnerable we are.

229           Now as we move to more of a smart grid, that also means  
230 that we have more vulnerabilities, whether it is from EMPs or  
231 from cyber attacks. So looking at how we can strengthen our  
232 ability to defend from these attacks is just part of our core  
233 effort here.

234           So at this time, I would like to yield the rest of my  
235 time to--

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

237 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
238           Mr. {Stearns.} The gentleman yields back the balance of  
239 his time?

240           Mr. {Terry.} Yes.

241           Mr. {Stearns.} And so we have extra time here, and we  
242 recognize Dr. Burgess for a minute and a half to 2 minutes.

243           Dr. {Burgess.} Thank you, Mr. Chairman for the  
244 recognition. I want to thank our witnesses for being here  
245 today, because this is an issue of extreme importance. We  
246 are facing threats from around the world, and certainly, all  
247 of us want to remain vigilant.

248           From hearings that we have had in previous Congresses in  
249 this Subcommittee, and from talking to people who are charged  
250 with protecting our country, defending our country in an  
251 increasingly adverse cyber environment, we are well aware  
252 that every day from around the world, as Mr. Terry mentioned,  
253 are trying to break into our vital modes of infrastructure  
254 and technology, and not the least of that being the electric  
255 grid.

256           We are also concerned about cost and that is why I am so  
257 grateful that some of the testimony today has focused on the  
258 effectiveness and the effectiveness of even the metrics that  
259 we use in order to assess how we are doing, and I think that  
260 is of critical importance, both as a consumer and certainly,

261 it is clear that the utility companies themselves will be  
262 interested in knowing what the effectiveness of the measures  
263 that we are asking them to implement--they have to be  
264 interested in the effectiveness of those measures.

265 We want these to be informed decisions. We do not want  
266 them to be emotional or political decisions, but we want them  
267 to be based on the best possible information, so that is why  
268 I am grateful, Mr. Chairman, that you called this hearing. I  
269 am grateful for our witnesses to be here, and I will yield  
270 back to the Chairman.

271 [The prepared statement of Dr. Burgess follows:]

272 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
273 Mr. {Stearns.} Gentleman yields back and we recognize  
274 the gentlelady from Tennessee, Ms. Blackburn--

275 Mrs. {Blackburn.} Thank you so much--

276 Mr. {Stearns.} --for a minute and a half.

277 Mrs. {Blackburn.} Thank you. I appreciate that. I do  
278 want to welcome our witnesses.

279 We all know and we realize how very--how debilitating  
280 these attacks would be. Some of the reports that I have read  
281 indicate that we could see blackouts for 9 to 18 months in  
282 areas if we were hit with a cyber attack, and certainly last  
283 year as we have looked at the series of attacks known as  
284 Night Dragon and how the hackers broke into and stole  
285 proprietary information worth millions of dollars, we see how  
286 this has a direct impact on not only U.S. but European energy  
287 companies.

288 I think that one of the things that concerns me is  
289 looking at what we have found out with the increase from '06  
290 to '10 a 650 percent increase in the number of attacks and  
291 the incidences that have been tracked. So we welcome you and  
292 we look forward to hearing what you have to say, and some of  
293 the accelerated planning issues that are in front of us.

294 Thank you very much. Yield back.

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

296 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
297           Mr. {Stearns.} Gentlelady yields back and I recognize  
298 the gentleman from Georgia, Mr. Gingrey, for 1 minute.

299           Dr. {Gingrey.} Mr. Chairman, I thank you for giving me  
300 a minute of time. I was looking for an e-mail on my iPhone,  
301 but I don't know how to use the iPhone so I couldn't pull up  
302 the e-mail. But basically I received an e-mail on my iPhone  
303 just a couple of days ago, purportedly from literally my best  
304 friend, who happens to be of European descent, and it was  
305 this typical e-mail, I am contacting you with tears in my  
306 eyes. We went on vacation in Spain, we got mugged at the--we  
307 can't get home, could you please e-mail us or wire us 1,600  
308 Euros? God bless you and thank you for your help. I mean,  
309 that kind of thing is amazing. It is the first time I have  
310 ever received one of those, but that is small potatoes, of  
311 course, compared to what we are talking about here, but it  
312 just is a small example of the seriousness of cyber attack on  
313 the smart grid, so I am really looking forward to hearing  
314 from the witnesses and learning more about this--

315           [The prepared statement of Dr. Gingrey follows:]

316 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
317 Ms. {DeGette.} Will the gentleman yield? Maybe your  
318 iPhone doesn't work because you opened that e-mail from your  
319 friend and now they have destroyed all your network.

320 Dr. {Gingrey.} I have been attacked.

321 Ms. {DeGette.} Yes.

322 Dr. {Gingrey.} Thank you, Ms. DeGette.

323 Ms. {DeGette.} You are welcome.

324 Mr. {Stearns.} All right, our side is complete. With  
325 that, recognize the Ranking Member of the Full Committee, the  
326 gentleman from California for 5 minutes.

327 Mr. {Waxman.} Thank you, Mr. Chairman. I appreciate  
328 your holding this hearing, and I want to say, this is exactly  
329 the type of oversight this Subcommittee should be conducting,  
330 ensuring that our government uses its resources wisely, and  
331 that the private sector is taking appropriate steps to  
332 guarantee the safety and security of our Nation's critical  
333 infrastructure.

334 Today's hearing will give us an opportunity to learn  
335 about the key challenges to ensuring the security of this  
336 Nation's electric grid. As the grid becomes more  
337 technologically advanced, it becomes more exposed to hackers,  
338 terrorists, and foreign enemies. As the grid becomes more  
339 interoperable, the potential effect of a cybersecurity breach

340 becomes more widespread.

341           The smart grid offers tremendous potential benefits.  
342 Modernizing the grid will make electricity cheaper, more  
343 efficient, more reliable, but at the same time, we must take  
344 appropriate action to protect the electric grid and to  
345 improve services and access for citizens across the Nation.

346           In 2007, Congress and then-President Bush approved the  
347 Energy Independence and Security Act of 2007. This  
348 legislation authorized the Smart Grid Investment Grant  
349 Program and the smart grid Demonstration Program. The 2009  
350 Recovery Act amended these programs and provided funding to  
351 ensure their implementation.

352           The first program, the Smart Grid Demonstration Program,  
353 funded 32 projects to verify the viability of smart grid  
354 technology and quantify the costs and benefits of these  
355 improvements. The second program, the Smart Grid Investment  
356 Grant Program, awarded grants for smart grid technology  
357 updates. These grants have allowed the installation of smart  
358 meters in millions of homes, implementation of automatic peak  
359 pricing, response for commercial and industrial customers,  
360 and the development of comprehensive demand response  
361 programs. These programs provided 99 grants to recipients in  
362 42 States, the District of Columbia, and Guam. In total, the  
363 Energy Department invested \$3.4 billion in grants, which was

364 matched by \$4.6 billion in private investments, for a total  
365 public private investment of over \$8 billion.

366 Today will give us an opportunity to evaluate what is  
367 working and what can be improved in these programs. The  
368 Department of Energy's Inspector General recently issued a  
369 report on the Smart Grid Grant Program and identified some  
370 reimbursement issues and concerns about approval of some  
371 cybersecurity plans. Today's hearing will allow us to  
372 explore those issues.

373 Beyond oversight, we must also do our part in protecting  
374 the electrical grid. Both GAO and the DOE Inspector General  
375 have acknowledged that Federal Energy Regulatory Commission  
376 has only limited authority to ensure the grid is truly  
377 secure. In fact, the Inspector General found that FERC does  
378 not have the authority to develop its own standards or  
379 mandatory alerts, even when new threats are identified. This  
380 gap in authority creates serious potential risks.

381 Last May, the Subcommittee on Energy and Power held a  
382 hearing to discuss the bipartisan Grid Reliability and  
383 Infrastructure Defense Act, a bill that would give FERC  
384 additional authority to protect the electric grid from  
385 potentially dangerous vulnerabilities. Today's hearing will  
386 again demonstrate why we need to act on this legislation  
387 without further delay. We must continue to invest in making

388 our electric grid the best in the world. That includes  
389 investing in standards and technologies so that the electric  
390 grid is secure in the face of unexpected terror attacks or  
391 hacking attempts. This hearing is an important step in  
392 identifying what can be done to ensure that the electric grid  
393 is protected.

394 I have focused my opening statement on the electric  
395 grid, but I hope this hearing produces some ways for members  
396 to learn how to use their iPhones, and to be able to realize  
397 that when they get e-mails asking for money, they had better  
398 think twice about it. I nearly fell for that one myself. A  
399 good friend was evidently not able to afford to leave Paris.  
400 Things could be worse, but they wanted something worse, they  
401 wanted my money. This shows that our security of our  
402 technology is very important objective, and I think it is  
403 worthwhile for our hearing to do it.

404 I am sure, since I have 19 second left, I want to  
405 comment that I am sure by the end of this hearing, whatever  
406 we find we don't like, the Republicans will blame on  
407 President Obama. Such is life. But I think this is a good  
408 hearing and I compliment the Chairman for holding it. I will  
409 yield back my second.

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

411 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
412 Mr. {Stearns.} The gentleman yields back his second,  
413 and I point out that sometimes we hear on your side  
414 everything is blamed on Bush, so--

415 Mr. {Waxman.} Too late for that.

416 Mr. {Stearns.} All right. Let me direct my comments to  
417 our witnesses this morning. As you know, the testimony that  
418 you are about to give is subject to Title 18 Section 1001 of  
419 the United States Code. When holding an investigative  
420 hearing, this Committee has a practice of taking testimony  
421 under oath. Do you have any objection to testifying under  
422 oath?

423 The Chair then advises you that under the rules of the  
424 House and the rules of this Committee, you are entitled to be  
425 advised by counsel. Do you desire to be advised by counsel  
426 during your testimony today? If not, would you please rise  
427 and raise your right hand?

428 [Witnesses sworn]

429 Mr. {Stearns.} You may now give your 5-minute summary  
430 of your written statement, and Mr. Wilshusen, you are first.

|  
431 ^TESTIMONY OF GREGORY C. WILSHUSEN, DIRECTOR OF INFORMATION  
432 SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE (GAO),  
433 ACCOMPANIED BY DAVID TRIMBLE, DIRECTOR, NATURAL RESOURCES AND  
434 ENVIRONMENT, GOVERNMENT ACCOUNTABILITY OFFICE (GAO); AND  
435 RICHARD J. CAMPBELL, SPECIALIST IN ENERGY POLICY,  
436 CONGRESSIONAL RESEARCH SERVICE (CRS)

|  
437 ^TESTIMONY OF GREGORY C. WILSHUSEN

438 } Mr. {Wilshusen.} Thank you, Mr. Chairman.

439 Chairman Stearns, Ranking Member DeGette, and members of  
440 the Subcommittee, thank you for the opportunity to testify  
441 today at today's hearing on cybersecurity for the smart grid.  
442 I am joined today by David Trimble, who is the Director for  
443 GAO's Natural Resources and Environment team. In addition,  
444 Mr. Chairman, if I may, I would like to recognize John  
445 Logoson, Mike Gilmore, and especially Lee McCracken for their  
446 efforts--

447 Mr. {Stearns.} Ask them to raise their hand. We are  
448 not sure--

449 Mr. {Wilshusen.} For their efforts in developing our  
450 written statement that we submitted today.

451 As you know, the electric power industry is increasingly

452 incorporating information technology systems and networks  
453 into its existing infrastructure as it modernizes the  
454 electricity grid. In 2007, the Energy Independence and  
455 Security Act established that it is federal policy to support  
456 this modernization. Known as a smart grid, these nationwide  
457 efforts are aimed at improving the reliability and efficiency  
458 of the grid, and facilitating the use of alternative energy  
459 sources. Smart grid technologies include smart meters that  
460 enable two way communications between utilities and  
461 customers, smart components that provide system operators  
462 with detailed data on the conditions of transmission and  
463 distribution systems, and advanced methods for controlling  
464 equipment. The use of these systems may have a number of  
465 benefits, such as fewer and shorter outages of electrical  
466 service, lower electricity rates, and an improved ability to  
467 respond to attacks on the electric grid.

468         However, the increased reliance on IT systems and  
469 networks also exposes the grid to cybersecurity  
470 vulnerabilities. For nearly a decade, GAO has identified the  
471 protection of systems supporting our Nation's critical  
472 infrastructures as--which include the electric grid--as a  
473 government-wide high risk area. Mr. Chairman, the threats to  
474 these systems supporting these infrastructures are evolving  
475 and growing. They include both unintentional and intentional

476 threats, and may come in the form of equipment failure, as  
477 well as targeted and untargeted attacks from our adversaries.

478         The interconnectivity between information systems, the  
479 internet, and other infrastructures can amplify the impact of  
480 these threats, potentially affecting the operations of  
481 critical infrastructures, the security of sensitive  
482 information, and the flow of commerce.

483         In January 2011, GAO reported on a number of key  
484 challenges to securing smart grid systems and networks. For  
485 example, the Federal Energy Regulatory Commission, or FERC,  
486 which has responsibility for adopting cybersecurity and other  
487 standards it deems necessary to ensure grid functionality and  
488 interoperability, had not developed a coordinated approach  
489 with other regulators to monitor industry compliance with  
490 voluntary standards. In addition, we reported other  
491 challenges affecting industry efforts to secure the smart  
492 grid. Specifically, the electricity industry had not  
493 consistently built security features under certain smart grid  
494 devices, established an effective mechanism for our sharing  
495 cybersecurity information, and created a set of metrics for  
496 evaluating the effectiveness of cybersecurity controls.

497         GAO made several recommendations to FERC aimed at  
498 addressing these challenges, and the Commission agreed with  
499 our recommendations.

500 To summarize, Mr. Chairman, the electricity industry is  
501 in the midst of a major transformation as a result of smart  
502 grid initiatives. While these initiatives hold the promise  
503 of significant benefits, including a more resilient electric  
504 grid, lower energy costs, and the ability to tap alternative  
505 sources of power, the prevalence of cyber threats aimed at  
506 the Nation's critical infrastructure and the cyber  
507 vulnerabilities arising from the use of new technologies  
508 highlight the importance of securing smart grid systems. In  
509 particular, it will be important for federal regulators and  
510 other stakeholders to work closely with the private sector to  
511 address key cybersecurity challenges posed by the  
512 transition--posed by the transition to smart grid technology.  
513 While no system can be made 100 percent secure, proven  
514 security strategies could help reduce risks to a manageable  
515 and acceptable level.

516 Chairman Stearns, Ranking Member DeGette, and other  
517 members of the Subcommittee, this completes my statement, and  
518 David and I would be happy to answer your questions.

519 [The prepared statement of Mr. Wilshusen follows:]

520 \*\*\*\*\* INSERT 1 \*\*\*\*\*

|  
521           Mr. {Stearns.} All right, and I understand, Mr.  
522 Campbell, your opening statement is welcome.

|  
523 ^TESTIMONY OF RICHARD J. CAMPBELL

524 } Mr. {Campbell.} Good morning, Chairman, Ranking Member,  
525 and members of the Subcommittee, my name is Richard Campbell.  
526 I am a Specialist in Energy Policy for the Congressional  
527 Research Service. On behalf of CRS, I would like to thank  
528 the Committee for inviting me to testify here today. I would  
529 like to request that my written testimony be entered into the  
530 record.

531 Mr. {Stearns.} By unanimous consent, so ordered.

532 Mr. {Campbell.} My testimony will provide background on  
533 the development of the smart grid, the Department of Energy's  
534 vision for the smart grid, and plans for the cybersecurity of  
535 the smart grid. I should note that CRS does not advocate  
536 policy or take a position on specific legislation.

537 The electrical grid in the United States comprises all  
538 of the power plants generating electricity, together with the  
539 transmission and distribution systems which bring power to  
540 end-use customers. The grid also connects the many public  
541 and private electricity companies and power companies  
542 throughout the United States. The modernization of the grid  
543 to accommodate today's power flows, serve reliability needs,  
544 and meet future projected uses is leading to the

545 incorporation of the electronic intelligence capabilities for  
546 power control and operations monitoring. The smart grid is  
547 the name given to this evolving intelligent electricity  
548 network. While these intelligent components may enhance the  
549 efficiency of grid operations, they also potentially increase  
550 the susceptibility of the grid to cyber, that is, computer-  
551 generated, attack, since they are built around microprocessor  
552 devices controlled by software programming. The potential  
553 for a major disruption or widespread damage to the Nation's  
554 power system from a large-scale cyber attack has increased  
555 focus on the cyber security of the smart grid.

556 The Department of Energy summarized its view of the  
557 potential of the smart grid by the year 2030 as a fully  
558 automated power delivery network that monitors and controls  
559 every customer and node, ensuring a two-way flow of  
560 electricity and information between the power plant and the  
561 appliance, and all points in between.

562 Federal funding has been provided to help develop  
563 concepts and technologies for the smart grid. The American  
564 Recovery and Reinvestment Act of 2009 provided \$4.5 billion  
565 in funding to the DOE for projects to modernize the grid.  
566 DOE's Smart Grid Investment Grant program received \$3.5  
567 billion of these funds with the expressed purpose of  
568 stimulating the rapid deployment of advanced digital

569 technologies needed to modernize the grid.

570         The SGIG is a cost-shared program, meaning recipients of  
571 grants were to provide as much as 50 percent of a project's  
572 total costs.

573         According to a recent report from the DOE's Office of  
574 Inspector General, all the available grant funds from the  
575 SGIG program have been awarded to 99 recipients, with awards  
576 ranging in value from \$397,000 to \$200 million. An approach  
577 to cybersecurity was required as part of the SGIG application  
578 process. Recipients of awards were required to submit a  
579 detailed plan addressing specific cybersecurity elements and  
580 concerns. The DOEIG report observed that DOE approved these  
581 cybersecurity plans even though weaknesses in the plans were  
582 identified and not fully addressed. The DOE responded to the  
583 report saying that it will require award recipients to update  
584 their cybersecurity plans later this year.

585         The DOE funded the development of the recently released  
586 Roadmap to Achieve Energy Delivery Systems Cybersecurity.  
587 This Roadmap provides a plan to improve the cybersecurity of  
588 the electricity, oil, and natural gas sectors.

589         The Roadmap recognizes the changing landscape of  
590 cybersecurity, and the continuing need to seek out and  
591 address cybersecurity gaps, and includes an implementation  
592 strategy for cybersecurity built on milestones to be achieved

593 by the year 2020.

594           The DOE has recently begun to update its vision for the  
595 smart grid, focusing on three key attributes it sees as  
596 desirable for the smart grid of the future: a seamless, cost-  
597 effective electricity system; a system capable of  
598 accommodating all generation choices; a system which enables  
599 customer choice.

600           According to this updated vision, the smart grid will  
601 still see regional diversity in power choices, while allowing  
602 for the development of a national framework. According to  
603 DOE, a reliable, secure, and resilient grid will be the key  
604 to achieving this vision.

605           In conclusion, it is the very features which can add  
606 seamless integration and utility to the smart grid that also  
607 add cyber vulnerabilities to electricity networks. Some  
608 assert that the smart grid and cybersecurity systems will  
609 have to develop along parallel but interconnected paths if  
610 the electric grid of the future is to develop in a manner  
611 that can enhance, and not impair, future economic  
612 development.

613           Congress could provide funding for research and  
614 development of systems to bridge gaps in cybersecurity and  
615 build the smart grid. Federal funding could also be used to  
616 bring government and industry together in forums to address

617 the needs and directions of these developing systems.

618 Congress may also provide for a regulatory framework  
619 which could achieve a basic level of cybersecurity. But due  
620 to the constantly changing nature of cyber threats, it is  
621 unlikely that effective cybersecurity of the grid will be  
622 achieved by regulation alone. Some assert that electric  
623 utilities must be focused on cybersecurity as keenly as they  
624 are on their current obligation to serve or to provide  
625 shareholder value.

626 Thank you for the invitation to appear today. I will be  
627 pleased to address any questions you may have.

628 [The prepared statement of Mr. Campbell follows:]

629 \*\*\*\*\* INSERT 2 \*\*\*\*\*

|  
630           Mr. {Stearns.} Thank you, Mr. Campbell. I will start  
631 with my questions.

632           Let us see if we get something that is current here. A  
633 2011 bulletin by the Department of Homeland Security titled  
634 ``Insider Threats to Utilities'' stated that ``based on the  
635 reliable reporting of previous incidents, we have a high  
636 confidence in our judgment that insiders and their actions  
637 pose a significant threat to the infrastructure and  
638 information systems of the United States facilities,'' vis-à-  
639 vis the grid. Mr. Wilshusen, are you aware of any specific  
640 power outage or threat to the electric grid that has  
641 transpired in such a way that is talked about in this  
642 Homeland Security report from 2011?

643           Mr. {Wilshusen.} You mean specifically from an insider  
644 threat?

645           Mr. {Stearns.} Yes.

646           Mr. {Wilshusen.} I can't say I know of a specific  
647 incident where that occurred; however, certainly insider  
648 threats are very important and a threat that our agencies and  
649 entities need to consider, because insiders typically have  
650 advanced knowledge and even access to the systems and the  
651 types of systems that contain information that they could  
652 have the ability then to perpetrate, if they have malicious

653 intent to cause disruptions and damage. And it is not just  
654 those with malicious intent, but also insiders who may be  
655 careless or who may be untrained that conduct activities that  
656 also impair or harm their systems and networks. But clearly,  
657 that is a key threat.

658 Mr. {Stearns.} Are you aware of any outsiders  
659 soliciting people in the smart grid viable areas? Are you  
660 aware of any outsiders that are trying to do this?

661 Mr. {Wilshusen.} In terms of corrupting--

662 Mr. {Stearns.} Yes.

663 Mr. {Wilshusen.} --and using insider threats? I can't  
664 say I know of specific examples of where that occurs--that  
665 occurred.

666 Mr. {Stearns.} Can you describe the controls and checks  
667 in place at utilities to prevent these kinds of attacks?

668 Mr. {Wilshusen.} Well, clearly one of the key controls  
669 that utilities and, indeed, agencies should do is background  
670 checks on their employees and those--

671 Mr. {Stearns.} Are they doing the background checks, in  
672 your opinion, adequately?

673 Mr. {Wilshusen.} We haven't examined the--how the  
674 securities are--

675 Mr. {Stearns.} So there has been no examination of how  
676 those background checks have been done and how they have been

677 corroborated, or the credibility of those checks?

678           Mr. {Wilshusen.} No, we have not assessed that as part  
679 of our review.

680           Mr. {Stearns.} Do you think that should be done?

681           Mr. {Wilshusen.} Well certainly it should be monitored  
682 and checked, because I do believe that individuals that have  
683 sensitive positions and hold--and have sensitive access to  
684 systems should have some level of background investigation  
685 performed. And there are other controls, too, that should be  
686 in place to help restrict and limit insiders, either careless  
687 or untrained insiders, as well as malicious from performing  
688 these types of acts, and that includes by limiting their  
689 access to only that level needed for them to perform their  
690 jobs, as opposed to giving them broader access to systems.

691           Mr. {Stearns.} The McAfee Corporation did a report in  
692 early 2011, another current report, in which they surveyed  
693 about 200 executives from critical electricity infrastructure  
694 across the United--across the world, in fact. That found  
695 that 85 percent had experienced network infiltrations, and 80  
696 percent had faced a large scale denial of service attack. Do  
697 you think that number is correct? That is quite large, 80  
698 percent of both network infiltrations and 80 percent faced a  
699 large scale denial of service attack. Do you think those  
700 figures are accurate?

701           Mr. {Wilshusen.} I have no basis to form whether they  
702 are accurate or not, but I will say as it relates to Federal  
703 Government agencies--

704           Mr. {Stearns.} Is that typical?

705           Mr. {Wilshusen.} In terms of those that have reported  
706 security incidents, yes, most federal agencies have done that  
707 and as the Congresswoman mentioned earlier, the number of  
708 reported security incidents within the Federal Government has  
709 risen by 650 percent from 2006 through 2010.

710           Now, what one disparity or inconsistency with that  
711 comment that you made, the statistics in that MacAfee report  
712 is that within the Federal Government, there was only about 1  
713 percent or so of the reported security incidents were  
714 considered to be denial of service attacks, which would be  
715 those that would disrupt the--

716           Mr. {Stearns.} So I assume you reviewed the MacAfee  
717 report yourself?

718           Mr. {Wilshusen.} No, I have not.

719           Mr. {Stearns.} How do these people get into cause these  
720 infiltrations? I mean, do you have any idea how it actually  
721 happens?

722           Mr. {Wilshusen.} Well, there are a number of different  
723 attack patterns--

724           Mr. {Stearns.} Just give me two quick, the most

725 prevalent.

726           Mr. {Wilshusen.} Well, one would be, for example, if  
727 they put malicious software on a thumb drive and then an  
728 employee of that corporation--

729           Mr. {Stearns.} Puts that thumb drive into the computer?

730           Mr. {Wilshusen.} Pardon?

731           Mr. {Stearns.} He puts that thumb drive in the  
732 software?

733           Mr. {Wilshusen.} Puts the thumb drive into the computer  
734 and then downloads the malicious software onto the computer.  
735 That is one way.

736           Mr. {Stearns.} To the hard disk, yes.

737           Mr. {Wilshusen.} Another way would be if the attacker  
738 would set up a malicious website and which would also then  
739 entice employees of the service center to--or wherever--to go  
740 to that website and download what appears to be an innocuous  
741 or an attractive program, when in fact, that too contains  
742 malicious code that could then allow--

743           Mr. {Stearns.} Could the facility put software in place  
744 to prevent both of those from occurring?

745           Mr. {Wilshusen.} They can, and disable certain  
746 functions--physical ports on the laptop or on the desktop to  
747 prevent that from happening. And indeed, the Department of  
748 Defense had such an attack on their networks based upon a

749 thumb drive that led them to disable the thumb drives on the  
750 vast majority of their--

751 Mr. {Stearns.} Last question. Has the Department of  
752 Homeland Security or the Department of Energy issued any  
753 guidance to the electricity sector on best practices that we  
754 just talked about in these two cases?

755 Mr. {Wilshusen.} Well, as part of the Energy  
756 Independence and Security Act, NIST, the National Institute  
757 of Standards and Technology, had responsibilities for  
758 developing security guidelines in connection with input from  
759 a number of different organizations that were then to be  
760 provided to FERC at Department of Energy to either approve if  
761 there is a consensus on those, and some of those controls  
762 would help to prevent such attacks, or could.

763 Ms. {DeGette.} Thank you. Mr. Wilshusen, were those  
764 controls, in fact, promulgated by FERC?

765 Mr. {Wilshusen.} No.

766 Ms. {DeGette.} Why not?

767 Mr. {Wilshusen.} It determined that there wasn't a  
768 consensus on those--development of those standards and  
769 cybersecurity guidelines, and under the Act, there--in the  
770 process are required to develop a consensus for--

771 Ms. {DeGette.} So now what? Are they developing  
772 standards?

773 Mr. {Wilshusen.} My understanding is that NIST is  
774 working to gain such a consensus.

775 Ms. {DeGette.} Okay. I want to talk with you a minute  
776 more about FERC, because what I am wondering is if they need  
777 extra authorities to protect the electric grid from these  
778 potentially dangerous vulnerabilities.

779 Can you just give us a quick example of the types of  
780 security flaws that might leave the grid vulnerable to  
781 hackers?

782 Mr. {Wilshusen.} One would be if they do not  
783 appropriately assess the risk to those various different  
784 components of the smart grid and implement the appropriate  
785 security controls over that. For example, if the access  
786 controls are not appropriately applied to different  
787 components of the grid, that could potentially allow a path  
788 into--

789 Ms. {DeGette.} And of course, the development of this  
790 smart grid increases this risk because it is more and more  
791 computerized, correct?

792 Mr. {Wilshusen.} Yes, the increased use of IT systems  
793 and networks provide additional paths and access points for  
794 potential attackers to gain access to it. In addition, the  
795 increasing interconnectivity of these systems and networks  
796 also allow potential attackers broader range and access to

797 other devices.

798 Ms. {DeGette.} And yet at the same time that there is  
799 broader vulnerability, the increased interconnection and the  
800 smart--development of the smart grid, it is a really valuable  
801 part of our system because it gives us--number one, it gives  
802 us more efficiency so consumers can get better prices, and  
803 number two, it allows us to use some of these renewable  
804 technologies that the Chairman was talking about in his  
805 opening statement, correct?

806 Mr. {Wilshusen.} Yes.

807 Ms. {DeGette.} And so here is my question. The GAO and  
808 others have said that there could be gaps in the FERC's  
809 regulatory authority to deal with development of these  
810 standards to respond to new vulnerabilities. Can you talk  
811 about that for a minute?

812 Mr. {Wilshusen.} Well in our recent report that we  
813 issued back in January of 2011, we identified that FERC did  
814 not have appropriate authorities, that their authorities were  
815 pretty much--since they didn't have the appropriate  
816 authorities, their authorities were limited to basically  
817 adopting and approving standards that were developed by  
818 others for the smart grid, and then primarily just at the  
819 bulk power level and bulk power supply level, not necessarily  
820 at the distribution level where certain smart grid

821 investments and devices are being implemented. And we made  
822 the recommendation to NERC that they need to really work with  
823 these other parties and stakeholders to include the State  
824 public utility commissions that do have such authorities and  
825 responsibilities to monitor the implementation of any  
826 standards that it adopts.

827 Ms. {DeGette.} So--

828 Mr. {Wilshusen.} And it had not done that.

829 Ms. {DeGette.} So do they have the authority to do  
830 that, or does Congress need to give them more authority to  
831 coordinate with those other operators?

832 Mr. {Wilshusen.} Well, they have the authority to  
833 coordinate with the other operators--

834 Ms. {DeGette.} Okay.

835 Mr. {Wilshusen.} --and utility commissions at the State  
836 level--

837 Ms. {DeGette.} Okay.

838 Mr. {Wilshusen.} --but they don't have the authority to  
839 mandate particular cybersecurity standards.

840 Ms. {DeGette.} Do you think they need that authority?

841 Mr. {Wilshusen.} We do not make that recommendation or  
842 really go there. We just actually made the recommendation to  
843 FERC that it determined whether, you know, what gaps overlaps  
844 exist, so--

845 Ms. {DeGette.} Yes, so if FERC determined that, they  
846 could come to us--

847 Mr. {Wilshusen.} Right.

848 Ms. {DeGette.} --and ask for that authority.

849 Mr. {Wilshusen.} That is correct.

850 Ms. {DeGette.} Now, there are some--do you know how  
851 many of these local and State authorities there are that FERC  
852 would need to be coordinating with?

853 Mr. {Trimble.} Well, you are--FERC is--

854 Ms. {DeGette.} Mr. Trimble?

855 Mr. {Trimble.} Yes, sorry.

856 Ms. {DeGette.} That is okay.

857 Mr. {Trimble.} FERC is--has jurisdiction over the bulk  
858 power system, but once it gets into the distribution system  
859 at the State level or at the local level, it falls to the  
860 State utilities. So the--

861 Ms. {DeGette.} There are thousands of them, right?

862 Mr. {Trimble.} Right, so you are talking about 50  
863 States plus those that aren't under State control or under  
864 minimal State control.

865 Ms. {DeGette.} Right, and then there is other agencies  
866 like Homeland Security, Energy and National Security Agency  
867 that also have oversight responsibilities over the critical  
868 electrical infrastructure, correct?

869 Mr. {Trimble.} Um-hum.

870 Ms. {DeGette.} So all of those individual utilities  
871 would have to work together to really address this, right?

872 Mr. {Trimble.} That is correct.

873 Ms. {DeGette.} Okay. Now, one last question, Mr.  
874 Chairman. I have got a lot more questions in this line, but  
875 maybe I will have an opportunity to ask then, but the Energy  
876 Independence and Security Act of 2007 directed the National  
877 Institute of Standards and Technologies to develop those  
878 standards, but those standards haven't been adopted for the  
879 reasons Mr. Wilshusen just explained, right?

880 Mr. {Trimble.} Right.

881 Mr. {Wilshusen.} That is correct.

882 Ms. {DeGette.} And do we have any sense when they are  
883 going to be adopted, now that it has gone back to the agency?

884 Mr. {Trimble.} We have not seen a timeline.

885 Ms. {DeGette.} Okay, thank you.

886 Mr. {Stearns.} The gentlelady from Tennessee is  
887 recognized for 5 minutes.

888 Mrs. {Blackburn.} I thank you all and appreciate so  
889 much the time that you are giving us today, and continuing to  
890 work with us through this issue.

891 I have found it so interesting, as we have worked  
892 through these hearings, how our constituents are paying

893 attention to this, and how they come back to us, those  
894 constituents that are working in informatics or in energy  
895 delivery systems, and they have different things they want to  
896 add to the discussion that we are having.

897         One question I do have on the smart meters that are out  
898 there. Is there a way that someone's proprietary information  
899 is being tracked or pulled or hacked into--what are the  
900 protections that are on these meters? Can you give me just a  
901 little bit of information on that, because some of our  
902 constituents--and Ms. DeGette talked about this when she said  
903 people can watch and find out when the electricity is going  
904 to cost them less and then do chores at that time, but our  
905 customers are saying now wait a minute. Is this--while it is  
906 giving me information, is this going to be giving--what are  
907 the protections, the privacy protections that are going to  
908 exist to the consumer about protecting that virtual presence  
909 and knowledge of themselves?

910         Mr. {Wilshusen.} Right, that is certainly an area of  
911 concern insofar as that those meters need to have the  
912 appropriate cybersecurity, information security controls  
913 built into them. We convened a panel of cybersecurity  
914 experts as part of our review that we issued a report back in  
915 January of 2011, and they identified that there are control  
916 deficiencies in some of those meters, to include not having

917 the appropriate login capabilities, which would help and--or  
918 the forensics capabilities to determine how and whether an  
919 attack had occurred.

920 Mrs. {Blackburn.} Okay, then let me ask you this. With  
921 those meters, would it be easy just to--is it very easy just  
922 to hack into them? Should people consider there to be so  
923 much transparency in these that they are not protecting their  
924 usage? Help me with that.

925 Mr. {Wilshusen.} Well, I would just say that it really  
926 depends upon the facts and circumstances of each individual  
927 type of meter--

928 Mrs. {Blackburn.} Okay.

929 Mr. {Wilshusen.} --and the security vulnerabilities or  
930 strengths relative to the individual meters.

931 Mrs. {Blackburn.} Okay. Mr. Wilshusen, I want to ask  
932 you, May '08 you made some comments about TVA's corporate  
933 network contains security weaknesses that could lead to  
934 disruption of their control systems, and of course, for those  
935 of us in the Tennessee Valley and TVA as the main power  
936 generator, we are very concerned about that. You had 19  
937 specific recommendations that you had for the TVA at that  
938 point in time. In your follow ons, has TVA implemented  
939 these? Have they been responsive to putting these controls  
940 in place? How are we doing with tightening that system up?

941 Mr. {Wilshusen.} Yes, TVA has been responsive in  
942 implementing not only the 19 recommendations that were made  
943 in the public report, but also we made a number of other  
944 recommendations in a limited distribution report--

945 Mrs. {Blackburn.} Exactly, yes.

946 Mr. {Wilshusen.} --that dealt more with the technical  
947 controls over their networks and their industrial control  
948 system networks. TVA has been responsive, has implemented  
949 most, if not all, of our recommendations and we have closed  
950 them out.

951 Mrs. {Blackburn.} Thank you. With that, I will yield  
952 back.

953 Mr. {Stearns.} Gentlelady yields back. Ms. Myrick is  
954 recognized for 5 minutes.

955 Mrs. {Myrick.} Thank you, and really, this is for any  
956 of you, but it concerns giving the cybersecurity threats and  
957 the weaknesses that were identified in the GAO report and in  
958 the Inspector General for the Department of Energy's report.  
959 It seems to be that cybersecurity is not a real high priority  
960 with some companies today, and given the wealth of  
961 information that is out there about the threats that exist--I  
962 am also on Intel and we deal with this all the time. And it  
963 just seems apparent to me that we--that companies really  
964 aren't taking this as seriously as they should. Not just

965 companies, of course, dealing with the electric grid, but  
966 other companies as well when it comes to how they fit into  
967 the big picture in the country.

968         Is it because they don't feel that there is any  
969 incentive for them to do it in any way? I am at a little of  
970 a loss, I guess, because some of them just seem to be kind of  
971 blasé about it, even though they are so vulnerable. It is  
972 unreal and then it affects the rest of us from a national  
973 security standpoint.

974         Mr. {Trimble.} I would answer in two ways. One, from  
975 our expert panel that we convened one of the concerns that  
976 they had was confusion and uncertainty over who is in charge  
977 in terms of--

978         Mrs. {Myrick.} Okay.

979         Mr. {Trimble.} --where the guidance was given, the  
980 complexity of the regulatory oversight. From--if you are  
981 putting yourself in the producer of the utilities  
982 perspective, they are faced with--so the standards haven't  
983 been adopted, even though--even when they are adopted, they  
984 are voluntary, and then if you are a producer under State  
985 control, you don't have anything from the States. To recover  
986 those costs, to make those investment decisions, those costs  
987 have to be recoverable. There is no necessary guarantee that  
988 you will recover those costs if you make those investments in

989 this uncertainty.

990           So again, this goes back to our recommendation as to  
991 when you adopt, you need to closely monitor to what extent  
992 these standards are being followed and to what extent they  
993 are effective, and make changes quickly. So it really, you  
994 know, sort of asking the system something it hasn't done  
995 necessarily in the past, which is act quickly and sort of  
996 more nimbly than it has. But I think part of the answer is  
997 really I would just put yourself in the shoes of the utility  
998 when faced with making those decisions and trying to balance  
999 the cost and benefits and risks that you are looking at.

1000           Mr. {Wilshusen.} And I want to add to that. Also in  
1001 some instances these utilities may or may not be fully aware  
1002 of some of the threats and risks that are there, particularly  
1003 certain incidents. In many cases, some of the most  
1004 actionable and alert information may not necessarily be able  
1005 to be shared with the utilities because it is classified.

1006           Mrs. {Myrick.} Right.

1007           Mr. {Wilshusen.} And so the information sharing  
1008 equation is also a factor in terms of the agency--or the  
1009 utilities receiving timely and actionable information.

1010           We issued a report a year ago or 2 years ago that dealt  
1011 with the expectations and the delivery of those expectations  
1012 between the public-private partnership model that is

1013 currently in use, and many--this is not only just the  
1014 electricity industry, but also across other critical  
1015 infrastructure sectors, in that most of the respondents on  
1016 the private sector side indicated that--in fact, 98 percent  
1017 of them said that receiving timely, actionable, alert and  
1018 threat information was very important to them, but only 27  
1019 percent of them responded and said that their federal  
1020 partners were greatly or moderately providing that  
1021 information to them.

1022 Mrs. {Myrick.} So it is not a resistance or lack of  
1023 understanding on the part of the companies from your  
1024 perspective and what you are seeing, it is really that they--  
1025 that this aspect of who is in charge and who they report to  
1026 and how they get the information and what information they  
1027 get is really the problem?

1028 Mr. {Wilshusen.} It is a contributing factor.

1029 Mrs. {Myrick.} Okay. Anybody else wish to comment?

1030 Then I yield back, Mr. Chairman. Thank you.

1031 Mr. {Stearns.} Gentlelady yields back. The gentleman  
1032 from Georgia, Mr. Gingrey, is recognized for 5 minutes.

1033 Dr. {Gingrey.} Thank you, Mr. Chairman, and I am going  
1034 to address my first question to all three of you, and I think  
1035 I will start with Mr. Campbell.

1036 Each of you mentioned in the January 2012 report issued

1037 by the Department of Energy's Inspector General that 36 of  
1038 the 99 grant recipients did not have the sufficient security  
1039 plans in place to provide further risk determent, despite the  
1040 fact that the Federal Government has spent, I think you said  
1041 \$3.5 billion in taxpayer money for this Smart Grid Investment  
1042 Grant Program. Now while I am disappointed that for  
1043 scheduling purposes it prevented the DOE Inspector General  
1044 from being here today, I would like to ask each of you your  
1045 thoughts on these three questions, and I will start with Mr.  
1046 Campbell. What are the potential implications of these  
1047 insufficient security controls?

1048 Mr. {Campbell.} Well basically smart grid devices are  
1049 being developed that may not have full cybersecurity  
1050 mechanisms built in. So if these devices do actually make it  
1051 to market, there could be problems with cybersecurity of the  
1052 devices going forward.

1053 Dr. {Gingrey.} Mr. Trimble?

1054 Mr. {Trimble.} Yeah, I will--what I would add to that,  
1055 and I will defer to my colleague on the cyber aspect of this,  
1056 that one of the downsides if you end up with devices that  
1057 don't meet the standards or aren't sufficiently protected and  
1058 then the utility has to pull those out, you have created a  
1059 problem in terms of who is going to pay for that mistake,  
1060 because they will go to the public utility to recover those

1061 costs, the public is not going to want to pay for the  
1062 mistake, and so you will have a very contentious situation.

1063       Mr. {Wilshusen.} Yeah, I would agree with both Mr.  
1064 Trimble and Mr. Campbell in that it could create  
1065 opportunities where key controls are not being implemented  
1066 into these devices or not being implemented in whatever the  
1067 initiative and grant initiative had was developing. One  
1068 thing that was noted by the IG is that these were approved  
1069 even though the Department had requested that the plans be  
1070 updated, which they were, but not in all instances were those  
1071 key controls addressed and the Department has to approve  
1072 that.

1073       According to the IG report, if I read that correctly--  
1074 again, I defer to the DOEIG on that--is that there was  
1075 apparently an emphasis on the part of the Department to make  
1076 sure that these grants were approved and gotten out.

1077       Dr. {Gingrey.} We--as the Chairman said in his opening  
1078 remarks, we had hoped to have the IG from DOE here today, and  
1079 hopefully we will schedule another hearing and hear from him.

1080       But going back to Mr. Campbell, throughout the life of  
1081 the grant, is it feasible that these problems that exist  
1082 could still be corrected?

1083       Mr. {Campbell.} The DOE's office has responded that it  
1084 will require the applicant grantees to update their

1085 cybersecurity plans, I believe it is by April of this year.

1086 Dr. {Gingrey.} All right, Mr. Trimble and Mr. W., you  
1087 all have some comments on that as well?

1088 Mr. {Wilshusen.} Yes. I would just also add that in  
1089 the report, the IG indicated that the Department was also  
1090 going to be, as part of their annual review process of these  
1091 grant initiatives, were to review the recipient's  
1092 implementation of those cybersecurity controls in their  
1093 plans.

1094 Dr. {Gingrey.} And then the last part of this question,  
1095 and I see I am probably only going to get one question in in  
1096 the allotted 5 minutes, but with this report in mind, the DOE  
1097 Inspector General report, do you know of any instances in  
1098 which the smart grid for which the grant program was supposed  
1099 to bolster has been compromised from a security standpoint?  
1100 Mr. Campbell, any specifics there?

1101 Mr. {Campbell.} I am not aware of any specifics.

1102 Dr. {Gingrey.} Mr. Trimble?

1103 Mr. {Trimble.} No, sir.

1104 Mr. {Wilshusen.} No, sir.

1105 Dr. {Gingrey.} Okay. I do have a little bit of time  
1106 left. Let me go--let us see, back to--well that is all  
1107 right. I will just save that if there is a second round.

1108 Mr. Chairman, I yield back the balance of my time.

1109 Mr. {Stearns.} All right, gentleman yields back. We  
1110 will do a second round and I will start.

1111 Mr. Wilshusen, in your testimony you stated that  
1112 Department of Energy Inspector General found that under the  
1113 Smart Grid Investment Grant Program, recipients were not  
1114 always complete or lacked sufficient detail in security  
1115 controls in their submissions to Department of Energy. Is  
1116 that correct?

1117 Mr. {Wilshusen.} Yes, sir.

1118 Mr. {Stearns.} Is that a big deal?

1119 Mr. {Wilshusen.} Yes, it can be.

1120 Mr. {Stearns.} And why, specifically?

1121 Mr. {Wilshusen.} Well, if those--

1122 Mr. {Stearns.} Why is it a big deal?

1123 Mr. {Wilshusen.} Well, if it is--

1124 Mr. {Stearns.} I think it is a big deal, but I just  
1125 want you to confirm it.

1126 Mr. {Wilshusen.} If those plans are incomplete and do  
1127 not identify key controls that should be implemented on as  
1128 part of these smart grid initiatives, that could lead to  
1129 vulnerable devices and therefore, may subject those devices  
1130 to increased risk of being compromised.

1131 Mr. {Stearns.} So you have a smart meter device being  
1132 purchased with government grant money that lacks the proper

1133 security features and if the guarantees don't have specific  
1134 or detailed security plans when installing them into the  
1135 customer's homes, isn't that it?

1136 Mr. {Wilshusen.} That could be a possibility.

1137 Mr. {Stearns.} Mr. Trimble, is it conceivable that  
1138 during the life of the grant period, that these security  
1139 plans are not complete, are not implemented properly, unless  
1140 made a condition of the grantee to receive the funding?  
1141 Should we do that?

1142 Mr. {Trimble.} I believe that should have been a  
1143 requirement or--

1144 Mr. {Stearns.} Do you have your mic on?

1145 Mr. {Trimble.} I believe that is what the IG indicated,  
1146 but that was not our work so I can't speak authoritatively.

1147 Mr. {Stearns.} Do you know of any specific examples  
1148 that I could hear from you, or Mr. Wilshusen?

1149 Mr. {Wilshusen.} Well in the IG report, they identified  
1150 three of the five security plans that it reviewed. These  
1151 were the plans that had already been initially identified by  
1152 the Department as having deficient or shortcomings in the  
1153 security programs, and then updated by the recipient or the  
1154 grantee recipients, and they identified that three of the  
1155 five still had the shortcomings and did not contain complete  
1156 information. And some of that information dealt, as I

1157 recall, with the auditing and some of the technical security  
1158 controls associated with those initiatives. But as far as  
1159 more detailed information, I did not review or have access to  
1160 the work papers supporting the report by the IG.

1161 Mr. {Stearns.} Is this all primarily in the smart meter  
1162 technology? Is that where all this concern is?

1163 Mr. {Wilshusen.} With the IG's report, I don't think it  
1164 was specific to that. I don't recall if it was specifically  
1165 mentioned.

1166 Mr. {Stearns.} Isn't that where most of the investment  
1167 is?

1168 Mr. {Wilshusen.} That also I don't know.

1169 Mr. {Stearns.} Yes, Mr. Trimble?

1170 Mr. {Trimble.} I believe it was in a broader range. I  
1171 thought the bulk of the money was into other systems like  
1172 phase measurement units and things like that, but again, we  
1173 haven't done work in that area.

1174 Mr. {Stearns.} Mr. Campbell, how many, in your opinion,  
1175 smart grid cyber incidents have there been?

1176 Mr. {Campbell.} I am not familiar with the total  
1177 number, but from I have heard in discussion there has been  
1178 quite a few cybersecurity incidents.

1179 Mr. {Stearns.} Under 10, under 100?

1180 Mr. {Campbell.} Probably more than that.

1181 Mr. {Stearns.} Under 1,000?

1182 Mr. {Campbell.} I couldn't say with any specific.

1183 Mr. {Stearns.} So you have no knowledge of how many  
1184 specific system cyber attacks there have been, incidents,  
1185 then?

1186 Mr. {Campbell.} No, sir.

1187 Mr. {Wilshusen.} Mr. Chairman--

1188 Mr. {Stearns.} Yes, sure.

1189 Mr. {Wilshusen.} --if I might add, I am not even sure  
1190 if there is a monitoring process or reporting mechanism in  
1191 place for that information to be reported and collected.

1192 Mr. {Stearns.} Mr. Campbell, do you think that waiting  
1193 3 years for the grant recipients to implement vigorous  
1194 cybersecurity plans could lead to cybersecurity gaps and  
1195 subsequent compromises in the system integrity?

1196 Mr. {Campbell.} It is my opinion--

1197 Mr. {Stearns.} If you might pull the mic just a little  
1198 closer.

1199 Mr. {Campbell.} It is my opinion that during the 3-year  
1200 period for development, there should be adequate time for the  
1201 DOE to take a look at the requirements in regard to  
1202 cybersecurity, but we should also note that cyber threats are  
1203 continuing to change, so any regulations that you may put in  
1204 place may not be adequate when the final product rolls out.

1205           Mr. {Stearns.} Okay. My last question, Mr. Wilshusen,  
1206 are there different cybersecurity challenges that are  
1207 vulnerabilities for government-run utility services, such as  
1208 the Bonneville Power Administration versus privately-run  
1209 utility services?

1210           Mr. {Wilshusen.} We haven't looked at the specific  
1211 security controls at private utilities. We have looked at  
1212 them at TVA, and identified a number of security  
1213 vulnerabilities--

1214           Mr. {Stearns.} At TVA?

1215           Mr. {Wilshusen.} At TVA, yes, as this was the report  
1216 that was referred to earlier. But my understanding is, it is  
1217 probably likely that what we found at TVA will probably be--  
1218 could be found at other public utilities as well, you know,  
1219 of a similar type of electrical power generation and some  
1220 transmission.

1221           Mr. {Stearns.} Mr. Trimble, anyone else, do you have  
1222 any comments in reference to the private versus government-  
1223 run utilities?

1224           Mr. {Trimble.} No, I would defer to Greg on that.

1225           Mr. {Stearns.} Mr. Campbell, any suggestions?

1226           Mr. {Campbell.} No, that seems to be a reasonable  
1227 response. Private utilities seem to have many of the same  
1228 systems that public utilities have.

1229 Mr. {Wilshusen.} And one--if I may just add more  
1230 broadly, when we looked at other sectors, for example, we  
1231 looked at communications network operated by private sector  
1232 organizations, we found vulnerabilities in their networks  
1233 that were similar to the vulnerabilities that we find in the  
1234 networks of federal agencies. Now while that is not exactly  
1235 electricity industry, but I would be fairly confident to say  
1236 that vulnerabilities identified in government systems are  
1237 going to probably be found in private sector systems in some  
1238 respects because the Federal Government security standards  
1239 and guidelines typically are as robust, if not more robust,  
1240 than private sector guidelines in many cases.

1241 Mr. {Stearns.} Thank you. My concluding comment is if  
1242 it hits one sector, it hit government utility versus private  
1243 utility, it is probably the same kind of statistic.

1244 Mr. {Wilshusen.} I would agree with that comment, which  
1245 is all the more reason why there should be an effective and  
1246 robust information sharing capability between the public and  
1247 private sectors.

1248 Mr. {Stearns.} With that, my time is expired.

1249 Ms. {DeGette.} Thank you. Thank you, Mr. Chairman.

1250 I want to follow up on the Chairman's question about  
1251 reporting, because I think I shared his concern. Mr.  
1252 Campbell and Mr. Wilshusen, both of you--all three of you

1253 said we don't have any kind of specific knowledge as to how  
1254 many cyber attacks there have been. And Mr. Wilshusen, you  
1255 said that we don't really have a systematic approach to  
1256 reporting. Would it be possible to develop that kind of  
1257 systematic approach, and if we did, how would it look, who  
1258 would be in charge of it, et cetera?

1259       Mr. {Wilshusen.} Well, we haven't done the work to come  
1260 up and just say definitively, but there are some reporting  
1261 mechanisms in place now. For example, the Department of  
1262 Homeland Security and the U.S. Cert federal agencies are  
1263 required to report their security incidents that occur at  
1264 their sites to U.S. Cert, and then U.S. Cert collects that  
1265 information and makes reports on it, summarizes it,  
1266 identified trends, and also then provides alerts to other  
1267 federal agencies.

1268       Private sector organizations can also report through to  
1269 the U.S. Cert, although in terms of having something formal  
1270 and required, that is--presently does not exist.

1271       Mr. {DeGette.} Well, so there is a structure that  
1272 perhaps you could do it, there is just no requirement to do  
1273 it, is that what you are saying?

1274       Mr. {Wilshusen.} It may be a model that could be  
1275 considered if one was to develop such a reporting structure.

1276       Ms. {DeGette.} Do you think it would be important to

1277 have some sense of incidences of cyber attacks?

1278 Mr. {Wilshusen.} Oh, I certainly do, yes.

1279 Ms. {DeGette.} What do you think, Mr. Campbell?

1280 Mr. {Trimble.} What I would--I am sorry, what I would  
1281 just jump in on this point is when we convened our expert  
1282 panel, one of the challenges and problems that the experts  
1283 identified was the lack of information sharing among the  
1284 utilities and the generators and the government on precisely  
1285 these issues, the cyber attacks, successful or not.

1286 Ms. {DeGette.} So did--so now we have identified--and  
1287 Mr. Campbell, would you agree there is a problem?

1288 Mr. {Campbell.} Yes, but I would also think  
1289 confidentiality of reporting would be a key factor in any  
1290 system that is developed.

1291 Ms. {DeGette.} Right, so who would develop that system?  
1292 I mean, we are super good at identifying problems, but now  
1293 how do we move towards a solution? Anyone?

1294 Mr. {Wilshusen.} Well, within the Federal Government,  
1295 you know, DHS has the overriding responsibility as the focal  
1296 point for protecting critical infrastructures. Each of the  
1297 18 critical sectors--infrastructure sectors have sector-  
1298 specific agencies that monitor it for that particular--

1299 Ms. {DeGette.} Yes, I understand all this, so you would  
1300 say it would probably be DHS to develop this?

1301           Mr. {Wilshusen.} They have a model in place where  
1302 federal agencies are required to. It would be a likely place  
1303 to start.

1304           Ms. {DeGette.} Okay, thank you.

1305           Mr. Campbell, I want to follow up on the point about  
1306 privacy that you just raised, because I don't know if the  
1307 three of you saw the story in ``The Washington Post'' today  
1308 where what it talked about was the National Security Agency  
1309 is pushing to expand its role in protecting private sector  
1310 computer networks from cyber attacks. The White House has  
1311 been concerned about privacy concerns, and then the story  
1312 said ``The most contentious issue was a legislative proposal  
1313 last year that would have required hundreds of companies that  
1314 provide such critical services as electricity generation to  
1315 allow their internet traffic to be continuously scanned using  
1316 computer threat data provided by the spy agency. Companies  
1317 would have been expected to turn over evidence of potential  
1318 cyber attacks by the government.'' So this really is an  
1319 issue about how you balance security versus privacy. We have  
1320 been debating this pretty much since September 11, 2001.

1321           And so maybe, Mr. Campbell, you can talk to me if you  
1322 have some perspective on the tradeoff of cybersecurity versus  
1323 privacy.

1324           Mr. {Campbell.} Well, I would say that cybersecurity

1325 versus privacy is a key issue. Other than that, I would say  
1326 that we--CRS is looking at the issue and we would be happy to  
1327 talk to you about it at a later time.

1328 Ms. {DeGette.} And you released--CRS released a report  
1329 on privacy and cybersecurity concerns earlier this month, did  
1330 it not?

1331 Mr. {Campbell.} Yes.

1332 Ms. {DeGette.} And so let me ask you, what information  
1333 can smart meters collect about the people in the households  
1334 who have them? I mean, what is the security issue?

1335 Mr. {Campbell.} Well, smart meters collect information  
1336 on the use of electricity, and so the idea is that smart  
1337 meters conceivably could develop a profile of the use of  
1338 electricity within the home. Now if the information is  
1339 accumulated at a high enough level, then individual use of  
1340 information could be lost, but that is an issue that is under  
1341 development and I think in various States there are various  
1342 rules concerning smart meter--

1343 Ms. {DeGette.} And that information, it could determine  
1344 the behavioral patterns of the residents in the home,  
1345 correct?

1346 Mr. {Campbell.} Correct.

1347 Ms. {DeGette.} So like burglar could figure out--could  
1348 use a smart meter to figure if a family was on vacation or

1349 not, right?

1350 Mr. {Campbell.} If they were sophisticated enough to  
1351 access the information.

1352 Ms. {DeGette.} Or a marketer could even use information  
1353 about what appliances a consumer might be using to target  
1354 that consumer, right?

1355 Mr. {Campbell.} Possibly.

1356 Ms. {DeGette.} So that--I mean, we wouldn't naturally  
1357 think that there would be security issues relating to these  
1358 meters, but that is something we need to consider and balance  
1359 out, right?

1360 Mr. {Campbell.} Correct.

1361 Ms. {DeGette.} Thank you, Mr. Chairman.

1362 Mr. {Stearns.} Gentleman from Georgia is recognized for  
1363 5 minutes.

1364 Dr. {Gingrey.} Thank you, Mr. Chairman.

1365 You know, as I sit here and think about this program and  
1366 the \$3.5 billion worth of grant money going towards these  
1367 companies, grantees, 99 of them to help develop the smart  
1368 grid, I also think about the \$19 billion that was in the  
1369 stimulus money for fully developing health information  
1370 technology, you know, the Offices of National Coordinator and  
1371 his salary and all the employees there to make sure that  
1372 people, companies small and large that got grants from that

1373 \$19 billion pot to help develop health information technology  
1374 that is fully coordinated, it just makes me concerned that  
1375 these grantees under this program to develop the smart grid  
1376 are not following the guidelines that they should follow and  
1377 in the final analysis 3 years from now we will have wasted a  
1378 lot of money.

1379 I want to ask you specifically, you mentioned--and maybe  
1380 some of my colleagues had asked a question about NIST's  
1381 involvement, the National Institute of Standards and  
1382 Technology, the 850-3 program as compared, let us say, to the  
1383 North American Electric Reliability Corporation's critical  
1384 infrastructure protection standards. Now how do those two  
1385 compare and are they overlapping? Are they similar? Is one  
1386 better than the other? What standards should we require of  
1387 these grantees as they develop these programs with taxpayer  
1388 money? Mr. Campbell?

1389 Mr. {Campbell.} My knowledge that the NERC reliability  
1390 critical infrastructure standards are just applied to those  
1391 on the bulk electric system, so when we are talking about the  
1392 Smart Grid Investment Grant Program, that is looking at  
1393 developing products, so I think what we are talking about is  
1394 two different types of requirements.

1395 Dr. {Gingrey.} Mr. Trimble and Mr. Wilshusen?

1396 Mr. {Wilshusen.} I will field that one. Also there is-

1397 -we actually compared the NERC's eight cyber--critical  
1398 infrastructure protections cybersecurity reliability  
1399 standards to the controls that are identified and NIST  
1400 Special Publication 850-3, and we found that of the 198  
1401 controls in 850-3 that the NIST or the NERC standards had  
1402 about 151 of those. One of the issues that the IG reported  
1403 on in its report, also in addition to what Mr. Campbell said,  
1404 is that those standards apply only to the bulk electricity  
1405 supply, but there further only apply to those assets that the  
1406 entities within that sector have designated as a critical  
1407 asset. And so if the entity has not identified any critical  
1408 assets, then those standards would not necessarily apply.

1409         And the IG report also indicated that back in 2009, the  
1410 former chief information security officer of NERC did a  
1411 survey and identified that about, I think it was 36 percent  
1412 of the power generators, or those entities with power  
1413 generation and about 67 percent of those responsible for  
1414 transmitting bulk power had identified only--at least one  
1415 critical asset. So that left a fair number of--or at least a  
1416 fair percentage of entities that produce power or transmit it  
1417 that did not identify any critical assets.

1418         Dr. {Gingrey.} Mr. Trimble?

1419         Mr. {Trimble.} I would just--my expertise is not cyber,  
1420 so I will--so to simplify that, the issue as I sort of have

1421 come to understand it is the NERC CIP standards apply to--for  
1422 critical infrastructure protection but it is limited because  
1423 it is just bulk power and it is just those that the industry  
1424 have identified as being critical assets. But industry self-  
1425 identification has not been exactly--has been identified as  
1426 comprehensively as it could be.

1427         The NIST standards that we are talking about for cyber  
1428 pursuant to ISA are voluntary, primarily focused on  
1429 interoperability and cyber threats. The limitation there is  
1430 that FERC's sort of bailiwick is, again, bulk power so it  
1431 doesn't get into anything beyond sort of interstate  
1432 transmission, if you will. If you are getting into the State  
1433 level, those guidelines, those standards, even though  
1434 voluntary, don't kick in. If you get down to the city level,  
1435 like New York, they don't kick in. So you have got this  
1436 patchwork where there is a whole bunch of places with no  
1437 standards that kick in.

1438         Dr. {Gingrey.} My time is expired, but I just want to  
1439 say that, you know, it is pretty much green eyeshades sort of  
1440 stuff, but hugely important, and of course, you are bringing  
1441 important information to us, the members of the Subcommittee,  
1442 and I think this is very beneficial. I deeply appreciate you  
1443 being here today, and thank you for your testimony.

1444         Mr. Chairman, I yield back.

1445 Mr. {Stearns.} Thank the gentleman and we are getting  
1446 ready to conclude the hearing, and I, as Chairman, have the  
1447 opportunity to give a closing remark. I would say it has  
1448 been brought up here and also I remember in our July hearing.  
1449 Department of Homeland Security fields all this information  
1450 dealing with cybersecurity and then gives it to U.S. Cert  
1451 agency, and they offer the documentation, as I understand it,  
1452 to the private industry, so it sort of filters down that way.  
1453 Is that correct?

1454 Mr. {Wilshusen.} I believe it is, yes.

1455 Mr. {Stearns.} Well, my concern is, just like the 9/11  
1456 Commission said, there was not full communication between all  
1457 the government agencies as well as private industries on  
1458 what--to alert them of possible information it could have  
1459 thwarted and stopped the 9/11 attack. I see it is clear here  
1460 today in the conversation that there is not really full  
1461 adequate communication between the private sector and the  
1462 government sector dealing with utilities with  
1463 cybersecurities, and I think this is a warning that we should  
1464 all take into effect or we might be sitting here at a later  
1465 date with something that is very serious.

1466 I want to thank the witnesses for their time and effort,  
1467 and the Subcommittee is adjourned.

1468 [Whereupon, at 11:37 a.m., the Subcommittee was

1469 adjourned.]