

**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 WITMER

3 HIF207.020

4 HEARING ON ``CYBERSECURITY: AN OVERVIEW OF RISKS TO CRITICAL  
5 INFRASTRUCTURE''

6 TUESDAY, JULY 26, 2011

7 House of Representatives,

8 Subcommittee on Oversight and Investigation

9 Committee on Energy and Commerce

10 Washington, D.C.

11 The subcommittee met, pursuant to call, at 11:00 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, Murphy,  
15 Burgess, Blackburn, Scalise, Griffith, DeGette, Schakowsky,  
16 Castor, Green, Christensen, and Waxman (ex officio).

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

19 Investigation; Karen Christian, Counsel, Oversight and  
20 Investigation; Alan Slobodin, Deputy Chief Counsel, Oversight  
21 and Investigation; Peter Spencer, Professional Staff Member;  
22 Carly McWilliams, Legislative Clerk; Andrew Powaleny, Press  
23 Assistant; Sean Bonyun, Deputy Communications Director;  
24 Kristin Amerling, Democratic Chief Counsel and Oversight  
25 Staff Director; Tiffany Benjamin, Democratic Investigative  
26 Counsel; Karen Lightfoot; Democratic Communications Director,  
27 and Senior Policy Advisor; and Ali Neubauer, Democratic  
28 Investigator.

|  
29           Mr. {Stearns.} Good morning, everybody. And the  
30 subcommittee will come to order. And I will start with my  
31 opening statement.

32           I have called to order this subcommittee's first hearing  
33 on cybersecurity and critical infrastructure protection.  
34 Over the last 15 years, our Federal Government has wrestled  
35 with the question of how best to protect our Nation's  
36 critical infrastructures from cyber attacks. Since September  
37 11, our infrastructure systems have become even more  
38 automated and more reliant on information systems and  
39 computer networks to operate. This has allowed our systems  
40 to become more efficient, but it has also opened the door to  
41 cyber threats and cyber attacks.

42           Recent reports and news articles have highlighted how  
43 threats and risks to cybersecurity have created  
44 vulnerabilities in our Nation's critical infrastructures and  
45 information systems. For example, just last week, the  
46 Department of Homeland Security sent out a bulletin about  
47 potential insider threats to utilities. That bulletin stated  
48 that outsiders have attempted to obtain information about the  
49 utilities' infrastructure to use in coordinating and  
50 conducting a cyber attack.

51           In March 2011, the computer systems of RSA were

52 breached. RSA manufactures tokens for secure access to  
53 computer networks. Sensitive information about these tokens  
54 was stolen and later used to hack into the network of  
55 Lockheed Martin, a Department of Defense contractor.

56 Last summer, the Stuxnet attack was identified. Stuxnet  
57 targets vulnerabilities in industrial control systems such as  
58 nuclear and energy to gain access to the systems and then  
59 manipulate the control process. This kind of attack has the  
60 potential to bring down or severely interrupt the functions  
61 of an electricity or even a nuclear plant.

62 The issues surrounding critical infrastructure  
63 protection and security are complex. Our systems are  
64 interconnected and depend on one other to operate. A  
65 vulnerability in one critical infrastructure naturally  
66 exposes other critical infrastructures to the same threats  
67 and risks, either because they are linked together through  
68 information systems or because one infrastructure depends on  
69 another to operate. In addition, much of the country's  
70 critical infrastructures are privately owned, as much as 80  
71 or 90 percent. They therefore have different operations,  
72 components, control systems, and computer networks--as well  
73 as vastly different resources available to address problems  
74 like cybersecurity and infrastructure protection.

75 My colleagues, we must identify and protect the very

76 systems that make our country run: energy, water, healthcare,  
77 manufacturing, and communications. Pursuant to the Homeland  
78 Security Act of 2002, DHS has led the coordination of  
79 infrastructure protection efforts with the private and public  
80 sectors and numerous federal agencies. One way DHS does this  
81 is to coordinate working groups and information sharing and  
82 analysis centers or ISACs in the individual critical  
83 infrastructure sectors and in cross-sector working groups.

84 DHS is primarily responsible for conducting threat  
85 analysis and issuing warnings about cyber threats so that  
86 other federal agencies and the owners and operators of  
87 critical infrastructure can simply protect their systems.  
88 DHS' efforts to protect our critical infrastructure have been  
89 the subject of some criticism.

90 Since 2003, the Government Accountability Office has  
91 designated ``protecting the Federal Government's information  
92 systems and the Nation's cyber critical infrastructures'' as  
93 a ``high risk'' area. In particular, in a report issued last  
94 July, GAO found that public- and private-sector owners and  
95 operators of critical infrastructure were not satisfied with  
96 the kind of cyber threat information they were getting from  
97 DHS. GAO has also expressed some concern that the sector-  
98 specific plans for dealing with cybersecurity need to be  
99 updated. In light of growing and more sophisticated cyber

100 attacks, this is obviously a critical issue.

101       As I mentioned previously, this is the subcommittee's  
102 first hearing in this Congress on critical infrastructure  
103 protection and cybersecurity. The purpose of this hearing in  
104 particular is to get an overview of DHS' role and  
105 responsibilities and how it coordinates with the sector-  
106 specific federal departments and agencies, many of which are  
107 subject to this committee's jurisdiction. Once we have a  
108 better understanding of DHS' role, it is my intention to call  
109 additional hearings to understand the issues that are  
110 presented in protecting the individual sectors, such as  
111 energy and information systems and communications.

112       Many ideas have been presented about how to improve  
113 critical infrastructure protection and cybersecurity. I  
114 believe the Oversight and Investigations Subcommittee has an  
115 important role to play in examining and bringing to light  
116 what is working now, and what can be done better.

117       I should note that this subcommittee's inquiry into this  
118 matter began with a bipartisan letter to the Department of  
119 Homeland Security asking for a briefing about its efforts to  
120 protect critical infrastructure. I appreciate the support of  
121 Ranking Member, Ms. DeGette, and the minority in this  
122 investigation. As Members of Congress, one of our foremost  
123 responsibilities is protecting our Nation's security and the

124 safety of its citizens.

125 With that I yield opening statement to the ranking

126 member, Ms. DeGette.

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

128 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
129           Ms. {DeGette.} Thank you very much, Mr. Chairman. And  
130 like you, this is a matter of great urgency. I am glad we  
131 are having this overview hearing and I am also happy to work  
132 with the majority on additional hearings in the particular  
133 issues of cybersecurity.

134           Just today, in the Washington Post it talked about a GAO  
135 report on significant breaches of classified computer  
136 networks in the Department of Defense. And while that is not  
137 in the jurisdiction of this committee, it just points out how  
138 vulnerable this country can be and why it is so important to  
139 keep our information systems safe.

140           The chairman referred to the cyber attack on RSA, which  
141 compromises the Department of Energy systems that  
142 necessitated shutting down internet connectivity for several  
143 days and breaches of Citibank data belonging to hundreds of  
144 thousands of customers. Anecdotally, at least, it seems like  
145 these breaches are becoming more and more frequent. The  
146 incidents remind us of the need for vigilance regarding  
147 efforts to prevent cybersecurity breaches and respond  
148 effectively when they occur and the importance of  
149 congressional oversight in these areas.

150           As the chairman mentioned, I asked him earlier this  
151 Congress to look into these issues, and I am really glad that

152 we are going to have a rigorous review of all of the  
153 cybersecurity issues. As the chairman mentioned, we have  
154 jurisdiction over a number of key components of our Nation's  
155 critical infrastructure, including the electrical grid,  
156 drinking water system, chemical plants, healthcare system,  
157 and telecommunications activities. In the last Congress, we  
158 saw progress in this committee regarding addressing  
159 cybersecurity issues in a number of these areas. The  
160 committee developed and passed on a bipartisan basis  
161 legislation to promote security and resiliency in the  
162 electrical power grid by providing the Federal Energy  
163 Regulatory Commission new authorities and providing for  
164 Department of Energy assistance to industry to protect the  
165 grid against cyber threats and other vulnerabilities. The  
166 committee also developed and passed legislation regarding  
167 chemical and drinking water facilities to meet the risk-based  
168 cybersecurity performance standards.

169 Cybersecurity issues are complex and evolving and  
170 deserve continuing and focused attention. One major question  
171 is how to best ensure an effective public-private partnership  
172 to address cybersecurity threats. The majority of our  
173 Nation's critical infrastructure is owned or operated by the  
174 private sector. While there are incentives for private-  
175 sector entities to protect the security of their information

176 networks, national security priorities may not always align  
177 with priorities and capabilities of the private sector.

178 I know that the Department of Homeland Security  
179 witnesses before us today are helping lead the  
180 administration's efforts to foster private- and public-sector  
181 cooperation in promoting cybersecurity and I look forward to  
182 hearing their insights on progress that is being made and  
183 obstacles that may still exist.

184 Another question we have to ask is how to best ensure  
185 that the Federal Government is drawing on its own expertise  
186 and experience to ensure cybersecurity measures are  
187 appropriately tailored to address specific needs in different  
188 critical infrastructure sectors. I look forward to hearing  
189 from GAO about these challenges. But even with a maximally  
190 effective partnership of federal agencies, state and local  
191 governments, and the private sectors in our country on  
192 cybersecurity protection, we must still address issues raised  
193 by the fact that information networks do not have national  
194 boundaries. Many reports suggested that the cyber attacks  
195 have started outside of American borders, raising serious  
196 questions about how we ensure international cooperation to  
197 protect against threats that cross borders. And in this DOD  
198 example, in the GAO report today, apparently the cyber attack  
199 came from a portable computer, a laptop computer that was

200 somehow tapped into.

201           And so I look forward to the insights of today's  
202 witnesses on these and other issues. I hope that we will  
203 build on this hearing with additional hearings on  
204 cybersecurity. It is one of the few bastions of  
205 bipartisanship left around here this week and I am happy to  
206 be part of it.

207           I yield back.

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

209 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
210 Mr. {Stearns.} I thank the gentlelady and recognize the  
211 gentleman from Texas, Dr. Burgess, for 2 minutes.

212 Dr. {Burgess.} I thank the chair.

213 To say that this committee has been working diligently  
214 for years is kind of an oxymoron but it does seem through  
215 several terms on this subcommittee we have indeed delved into  
216 this issue. I am anxious that we bring this to a legislative  
217 conclusion and institute those things that will provide the  
218 protection that I think we all feel that we need. There are  
219 critical urgent things that need to be done to protect our  
220 transmission grid, our power plants from attacks from those  
221 who wish to do us harm. The threats are real. It is time to  
222 move the legislation forward.

223 We do have to be careful that we don't unduly shift the  
224 balance of responsibility that has been properly maintained  
225 between the government and the private sector for decades.  
226 It is important that we be careful; it is important that we  
227 be prudent in providing the Federal Government any additional  
228 authority. If indeed any is necessary, it must be done in a  
229 way that cannot be abused and will not result in  
230 significantly higher cost to consumers and businesses at a  
231 time when the economy is so fragile. And it must not result  
232 in the loss of any personal freedoms that people now have.

233           The testimony we will hear today will help this  
234 committee in perfecting legislation that was considered last  
235 year. I certainly look forward to working with members on  
236 both sides of the dais to ensure that the legislation is  
237 mindful of both the real threats that we face and the burdens  
238 that granting new powers to the Federal Government can  
239 create. Ensuring this balance can and should be done.

240           Thank you, Mr. Chairman, for the recognition. I will  
241 yield back my time.

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

243 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
244           Mr. {Stearns.} The gentleman yields back and the  
245 gentlelady from Tennessee, Ms. Blackburn, is recognized for 2  
246 minutes.

247           Mrs. {Blackburn.} Thank you, Mr. Chairman. And I want  
248 to welcome our witnesses. We appreciate that you would take  
249 the time and come over here to the Hill. We all do know and  
250 do agree that cybersecurity is an important issue and we know  
251 that there are those who are, as we speak, waging war if you  
252 will on our vital infrastructure.

253           Last month, Wall Street Journal reported that the IMF  
254 was investigating a recent cyber attack. Not surprisingly,  
255 this attack came just 1 month after a group called Anonymous  
256 indicated its hackers would target the IMF website in  
257 response to the strict austerity measures in its financial  
258 package of Greece.

259           Closer to home, in my State of Tennessee, presides our  
260 Nation's largest public power utility, the Tennessee Valley  
261 Authority. TVA's power networks stretch across 80,000 square  
262 miles in the Southeastern U.S. and provide electricity to  
263 more than 8.7 million Americans. Under Homeland Security  
264 Presidential Directive number 7, TVA is considered a National  
265 Critical Infrastructure and must take great steps to protect  
266 and to safeguard its essential cyber assets. A power grid

267 disruption or other threat on TVA operations or any other  
268 public utility in our country would cause a cascading effect  
269 impacting our economy, safety, and daily lives.

270           In fact, this concern was reaffirmed last month as  
271 former CIA director and current Secretary of Defense Panetta  
272 appeared before the Senate Armed Services Committee and  
273 declared that the next Pearl Harbor our Nation confronts  
274 could very well be a cyber attack that cripples our power  
275 systems, the grid, our security systems, our financial  
276 systems, and our governmental systems.

277           With all that in mind, I thank the chairman for the  
278 hearing. I thank you all for your participation as we  
279 discuss what steps DHS is taking to avoid what would be the  
280 unimaginable, a Pearl Harbor attack on our Nation's vital  
281 infrastructure.

282           And I yield back.

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

284 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
285           Mr. {Stearns.} The gentlelady yields back and I  
286 recognize Ms. Christensen from the Virgin Islands for 5  
287 minutes.

288           Dr. {Christensen.} Thank you, Chairman Stearns, and  
289 thank you, Ranking Member DeGette, for holding this hearing  
290 to discuss cybersecurity risks, threats, and challenges to  
291 our Nation's critical infrastructure. Many of today's  
292 battles are in cyberspace where terrorism and hackers help  
293 attack our cell phones, computer grids, and have the  
294 potential to destroy sensitive information in 18 of our  
295 Nation's most critical sectors.

296           Since 9/11, we have known to expect that we would  
297 experience terrorist attacks that would be cyber attacks. As  
298 a former member of the Homeland Security Committee, I have  
299 taken part in many hearings and worked on legislation  
300 addressing this issue. As our witnesses who we welcome here  
301 today will testify, a lot has been done to create entities to  
302 coordinate and oversee efforts to address and prevent  
303 cybersecurity threats. But there are still challenges to  
304 protecting our Nation's infrastructure from these threats and  
305 we must continue to examine how we can overcome these  
306 challenges.

307           In doing so, it is important that we pass legislation to

308 protect our Nation's electric grid. All of these long-term  
309 initiatives require a national electric grid that is reliable  
310 and secure. The electrical grid serves more than 143 million  
311 American customers, has to operate without interruption, and  
312 is a key foundation of our national security. Designing and  
313 operating an electrical system that prevents cybersecurity  
314 events from having a catastrophic impact is a challenge we  
315 must all address. And I want to add that the healthcare  
316 sector is not immune to these attacks either.

317         So I would like to thank DHS and GAO and commend both  
318 Agencies for their efforts to address imminent cybersecurity  
319 threats. And with that, I will yield back the balance of my  
320 time.

321         [The prepared statement of Dr. Christensen follows:]

322         \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
323 Mr. {Stearns.} The gentlelady and yields back.

324 And at this time, we will move to our first panel, our  
325 witnesses. Let me address you folks.

326 You are aware that the committee is holding an  
327 investigative hearing and when doing so has had the practice  
328 of taking testimony under oath. Do you have any objections  
329 to taking testimony under oath? All right. No.

330 The chair then advises you that under the rules of the  
331 House and the rules of the committee you are entitled to be  
332 advised by counsel. Do you desire to be advised by counsel  
333 during your testimony today? All right.

334 In that case, if you will please rise and raise your  
335 right hand, I will swear you in.

336 [Witnesses sworn.]

337 Mr. {Stearns.} You are now under oath and subject to  
338 the penalties set forth in Title XVIII, Section 1001, of the  
339 United States Code.

340 We welcome the three of you for your 5-minute summary  
341 statement. And we have Ms. Bobbie Stempfley, Acting  
342 Secretary of the DHS Office of Cybersecurity and  
343 Communications, welcome; and Mr. Sean P. McGurk, Director,  
344 National Cybersecurity and Communications Integration Center  
345 in the Office of Cybersecurity and Communications at DHS; and

346 lastly, Mr. Gregory Wilshusen, Government Accountability  
347 Office Director of Information Security Issues. Thank you.

348 And Ms. Stempfley, we welcome your opening statement.

349 Just turn the mike on if you don't mind. Just move it close  
350 to you so we can hear you. That would be super. Thanks.

|  
351 ^TESTIMONIES OF ROBERTA STEMPFLEY, ACTING ASSISTANT  
352 SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS,  
353 NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF  
354 HOMELAND SECURITY; SEAN P. MCGURK, DIRECTOR, NATIONAL  
355 CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, OFFICE  
356 OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND  
357 PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY; AND  
358 GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES,  
359 GOVERNMENT ACCOUNTABILITY OFFICE

|  
360 ^TESTIMONY OF ROBERTA STEMPFLEY

361 } Ms. {Stempfley.} Okay. Thank you very much. So thank  
362 you very much, Chairman Stearns, Ranking Member DeGette, and  
363 other members of the subcommittee.

364 As you heard, my name is Bobbie Stempfley, and I am the  
365 acting assistant secretary in the Office of Cybersecurity and  
366 Communications at the Department of Homeland Security, and it  
367 is definitely my privilege to be here to speak to you today  
368 with my colleagues from across government to talk about  
369 cybersecurity, which is an area of great passion for all of  
370 us.

371 The opening comments did such a wonderful job describing

372 the threat landscape that we operate in today. It certainly  
373 is one we have increasing sophistication, increasing  
374 severity, and an environment where no one is immune from  
375 individuals to private-sector companies, and one where we see  
376 it slightly untenable where the threat actors have to make  
377 one right choice in an environment where only a single wrong  
378 implementation in the networks that are being defended  
379 enables access. And so it is an environment where we spend a  
380 great deal of time bringing together private-sector partners  
381 and others.

382 We have identified 38,000 vulnerabilities over a period  
383 of time in critical infrastructures and provide warning  
384 notification and awareness products around those  
385 vulnerabilities to private-sector individuals. It is an  
386 environment, as the chairman pointed out, of significant  
387 interdependence, both between critical infrastructure  
388 sectors, between corporations, between environments. Several  
389 examples that you provided do a wonderful job illuminating  
390 that interdependence across the board. And that means that  
391 it requires an interdependent and integrative approach in  
392 order to provide protective, preventative, and restoral and  
393 defensive measures both across government and within the  
394 private sector.

395 It is the job of the National Protection and Programs

396 Directorate; it is our mission responsibility to secure the  
397 federal executive civilian branch--that is the federal  
398 departments and agencies--to provide technical support to  
399 private-sector individuals, owners, and operators to help  
400 them with risk assessment, with mitigation, with restoral and  
401 response activities. It is also our mission to provide  
402 general awareness to the broad public. And finally, as Mr.  
403 McGurk will discuss, to provide national coordination and  
404 response across the board.

405         It is, as I said, not an environment where a single  
406 solution works or a single organization provides all of the  
407 answers. It is an environment where much progress has been  
408 made and it is a team sport for us all. Cooperation between  
409 law enforcement, between intelligence agencies, between the  
410 Homeland Security, between, as I said, government and private  
411 sector is a significant part of how we need to move forward  
412 of the successes we have had to date.

413         Examples such as you pointed out, the compromise in RSA  
414 really helps demonstrate the progress that has been made in  
415 government. The response that we had in that worked across a  
416 set of responsibilities defined in the National Cybersecurity  
417 Instant Response Plan where law enforcement has  
418 responsibility for pursuit and for investigation, where  
419 intelligence has warning responsibilities and attribution

420 responsibilities, and where Homeland Security's  
421 responsibilities are in protection, prevention, restoral, and  
422 response. And that partnership across government is so  
423 important for us as we work through each of the events that  
424 occur.

425         We have in a proactive manner responded to 100 requests  
426 from critical infrastructure partnerships, largely across  
427 water, oil, and gas and power to help identify  
428 vulnerabilities in their environment and help them improve  
429 the capabilities that they have for protection and for  
430 response. It is through that partnership that we continue to  
431 work to enhance our prevention activities because, as we  
432 said, we are in that untenable environment today.

433         What we have also put a great deal of effort in is to  
434 increase visibility and information sharing across  
435 environments. Again, I look forward to the comments of Mr.  
436 McGurk in our operations center. But it is information  
437 sharing not only in operations and in response, but  
438 information sharing at large that is important across the  
439 board.

440         And so in conclusion, I look forward to further  
441 questions from the committee to discuss what we have done.  
442 And it, again, is my pleasure to be here today.

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

444 \*\*\*\*\* INSERT 1 \*\*\*\*\*

|

445 Mr. {Stearns.} Thank you.

446 Mr. McGurk, you are welcome for your opening statement.

|  
447 ^TESTIMONY OF SEAN P. MCGURK

448 } Mr. {McGurk.} Thank you, Chairman Stearns, Ranking  
449 Member DeGette, and distinguished members of the  
450 subcommittee. My name is Sean McGurk. I am the director of  
451 the National Cybersecurity and Communications Integration  
452 Center, also known as the NCCIC. Thank you for inviting me  
453 here today along with my distinguished colleagues to discuss  
454 the overall cyber-risk to critical infrastructure. The  
455 Department greatly appreciates the committee's support for  
456 our central mission and looks forward to working with the  
457 committee to establish the necessary plans and programs  
458 moving forward to address risks to the critical  
459 infrastructure.

460 The cyber environment is not homogenous under a single  
461 department or agency nor under the private sector. Each of  
462 the 18 critical infrastructure and key resource sectors are  
463 completely different--energy, water, nuclear, transportation,  
464 they all have their unique challenges and their unique  
465 environments. In fact, within a particular company, two  
466 plants may not have the same operating environment. We rely  
467 on this continuous availability of a vast, interconnected,  
468 critical infrastructure to sustain our way of life. A

469 successful cyber attack could potentially result in physical  
470 damage and even loss of life. We face a significant  
471 challenge moving forward--strong and rapidly expanding  
472 adversary capabilities and a lack of comprehensive threat and  
473 vulnerability awareness.

474 Support of these efforts from our private-sector  
475 partners is key to securing these critical infrastructures.  
476 The government does not have all the answers, so we must work  
477 with the private sector to establish those guidelines. There  
478 is no one-size-fits-all solution in a cyber environment.  
479 There is no cyber Maginot Line. We must leverage our  
480 expertise and our access to information, along with industry-  
481 specific needs, capabilities and timelines. Each partner has  
482 a role and a unique capability, as demonstrated by the  
483 diversity of this panel.

484 Two-factor authentication was mentioned earlier, the RSA  
485 example. In that particular example, within a 24-hour  
486 period, the Department, working along with law enforcement  
487 and with the intelligence community, responded to a request  
488 from the private industry partner to provide a mitigation,  
489 identification, and assessment team in support of their  
490 mitigation efforts. The Department continuously works with  
491 our private-sector partners and the financial-services  
492 sector, energy sector, communications, IT, and others to

493 prepare, prevent, respond, recover, and restore.

494         Coordinating the national response of domestic cyber  
495 emergencies is the focus of the National Cyber Incident  
496 Response Plan and indeed the NCCIC. The what and the how on  
497 the cyber attack is the focus and the intent of our  
498 mitigation activities. The who and the why usually come  
499 later.

500         The NCCIC works closely with the government at all  
501 levels and private sector to coordinate and integrate a  
502 unified cyber response. Sponsoring security clearances for  
503 our partners enable them to participate fully in our watch-  
504 center environment. To date, we have physical representation  
505 from the communications sector and its Information Sharing  
506 and Analysis Center and also with companies such as AT&T,  
507 Verizon, and Sprint. The information technology sector is  
508 represented physically on the watch floor along with the  
509 financial-services sector, NERC, representing the North  
510 American Energy Reliability Corporation; representing the  
511 energy sector, Information Sharing and Analysis Center; and  
512 most recently, we have begun to coordination and share  
513 information with the National Electric Sector Cybersecurity  
514 Organization, or NESCO.

515         We have virtual connections as well as physical  
516 connections with these organizations and we share data in

517 near-real time. Additionally, we have a physical  
518 representative from the Multi-State ISAC, enabling us to  
519 provide actionable intelligence to state, local, tribal, and  
520 territorial governments and their representatives. Each of  
521 these partners bring a unique perspective and a unique  
522 capability to the watch environment.

523         Currently, within our legal authorities, we continue to  
524 engage, collaborate with our partners and provide analysis,  
525 vulnerability, and mitigation assistance to the private  
526 sector. We have experience and expertise in dealing with the  
527 private sector in planning steady-state and crisis scenarios.  
528 We have deployed numerous incident-response teams and  
529 assessment teams that enable us to prevent and to respond,  
530 recover, and restore to cyber impacts.

531         Finally, we work closely with the private sector and our  
532 interagency partners and law enforcement and intelligence to  
533 provide the full complement of capabilities from the federal  
534 standpoint in preparation for and response to significant  
535 cyber incidents.

536         Chairman Stearns, Ranking Member DeGette, and  
537 distinguished members of the subcommittee, let me conclude by  
538 reiterating that I look forward to exploring opportunities to  
539 advance the mission and collaboration with the subcommittee  
540 and my colleagues in the public and private sector. Thank

541 you again for this opportunity to testify and would be happy  
542 to answer your questions.

543 [The prepared statement of Mr. McGurk follows:]

544 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
545           Mr. {Stearns.} Thank you. Mr. Wilshusen?

|  
546 ^TESTIMONY OF GREGORY C. WILSHUSEN

547 } Mr. {Wilshusen.} Chairman Stearns, Ranking Member  
548 DeGette, and members of the subcommittee, thank you for the  
549 opportunity to testify in today's hearing on the  
550 cybersecurity risks to the Nation's critical infrastructure.  
551 But before I begin, if I may, Mr. Chairman, I would like to  
552 recognize Mike Gilmore, Tammy Carvette, and Lee McCracken,  
553 who is sitting behind me, and also Brad Becker from our  
554 Denver office, who are responsible for the significant  
555 contributions in reviewing this area and helping me prepare  
556 this testimony today.

557 Mr. {Stearns.} I am glad you did. Thank you.

558 Mr. {Wilshusen.} Critical infrastructures are systems  
559 and assets, whether physical or virtual, so vital to our  
560 Nation that their incapacity or destruction would have a  
561 debilitating effect on our national security, economic  
562 wellbeing and public health and safety. They include, among  
563 other things, banking and financial institutions,  
564 telecommunications networks, and energy production  
565 transmission facilities, most of which are owned by the  
566 private sector. These infrastructures have become  
567 increasingly interconnected and dependent on interconnected

568 networks and systems. And while the benefits of this  
569 interconnectivity have been enormous, they can also pose  
570 significant risk to the networks and systems, and more  
571 importantly, to the critical operations and services they  
572 support.

573 In my testimony today, I will describe the cyber threats  
574 confronting critical infrastructures, recent actions by the  
575 Federal Government to identify and protect these  
576 infrastructures and ongoing challenges to protecting them.

577 Mr. Chairman, our Nation's critical infrastructures face  
578 a proliferation of cyber threats. These threats can be  
579 intentional or unintentional. Unintentional threats can be  
580 caused by equipment failures, software upgrades, or  
581 maintenance procedures that inadvertently disrupt the  
582 systems. Intentional threats include both targeted and non-  
583 targeted attacks from a variety of sources, including  
584 criminal groups, hackers, insiders, and foreign nations  
585 engaged in intelligence gathering and espionage.

586 First, recent reports of cyber attacks incidents  
587 involving cyber-reliant critical infrastructure underscore  
588 the risks and illustrate that they can be used to disrupt  
589 industrial control systems and operations, commit fraud,  
590 steal intellectual property and personally identifiable  
591 information, and gather intelligence for future attacks.

592 Over the past 2 years, the Federal Government has taken a  
593 number of steps aimed at addressing cyber threats and better  
594 protecting critical infrastructures.

595 For example, a cyberspace policy review identified 24  
596 recommendations to address the organizational and policy  
597 changes needed to approve the current U.S. approach to  
598 cybersecurity. DHS updated the National Infrastructure  
599 Protection Plan in part to provide a greater focus on cyber  
600 issues and issued an interim version of the National Cyber  
601 Incident Response Plan. It also conducted Cyber Storm III, a  
602 cyber attack simulation exercise intended to test elements of  
603 the National Response Plan.

604 In addition, DHS, as you know, created the National  
605 Cybersecurity and Communications Integration Center, or  
606 NCCIC, to coordinate national response efforts, as well as  
607 work directly with other private- and public-sector partners.

608 Despite these threats, more needs to be done to address  
609 a number of remaining challenges. For example, implementing  
610 the recommendations made by the President's Cybersecurity  
611 Policy Review, updating the national strategy for securing  
612 the information and communications infrastructure,  
613 strengthening the public-private partnerships for securing  
614 cyber-reliant critical infrastructures, enhancing cyber  
615 analysis and warning capabilities, and securing the

616 modernized electricity grid.

617           In summary, the threats to information systems are  
618 evolving and growing and systems supporting our Nation's  
619 critical infrastructures are not yet sufficiently protected  
620 to consistently thwart the threats. While actions have been  
621 taken, federal agencies and partnership with the private  
622 sector need to act to improve our Nation's cybersecurity  
623 posture, including enhancing cyber analysis and warning  
624 capabilities and strengthening the public-private  
625 partnerships. Until these actions are taken, our Nation's  
626 critical infrastructure will remain vulnerable.

627           Mr. Chairman, this concludes my statement. I would be  
628 happy to answer any questions for you or other members of the  
629 subcommittee.

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

631 \*\*\*\*\* INSERT 2 \*\*\*\*\*

|  
632 Mr. {Stearns.} I thank the gentleman.

633 Let me ask you a question. I have your opening  
634 statement here in which you mention various cybersecurity  
635 attacks. They are putting software viruses into the network.  
636 Is that primary what it is?

637 Mr. {Wilshusen.} It could be a number of different  
638 attacks. In terms of one to include computer intrusions in  
639 which individuals are able to gain access through the  
640 installation of malicious software. For example, if a user  
641 inadvertently plugged a USB into his computer that was  
642 corrupted, it could install some malicious software, which  
643 might facilitate an attack.

644 Mr. {Stearns.} Now, when an attack occurs--

645 Mr. {Wilshusen.} Um-hum.

646 Mr. {Stearns.} --generally, what does that attack look  
647 like? They are coming in to steal information, or are they  
648 coming to put in a replicating software that will destroy it,  
649 or is it just putting in there to observe? What of those  
650 three?

651 Mr. {Wilshusen.} It could be any of the combinations.

652 Mr. {Stearns.} Any of those three combinations?

653 Mr. {Wilshusen.} Right. One, in terms of either to  
654 sabotage his particular system or gain information for future

655 attacks perhaps or as well to--

656 Mr. {Stearns.} Depending upon their motivation.

657 Mr. {Wilshusen.} Depending upon their motivation.

658 Mr. {Stearns.} Mr. McGurk, what do you think?

659 Mr. {McGurk.} Yes, sir. I would also echo my  
660 colleague's statements that the vast array of capability we  
661 see demonstrated with the malicious code is such that it  
662 encompasses all of those things.

663 Mr. Chairman, you had mentioned Stuxnet earlier. That  
664 is a great example of a particular piece of malicious code  
665 that demonstrated very unique capabilities. It not only  
666 exploited what we call zero-day vulnerabilities, which are  
667 vulnerabilities that are not known in the public environment,  
668 but also it used advanced communication capability. It did  
669 advanced reconnaissance, so it was gathering information.  
670 And subsequently, it left behind that malicious code that was  
671 able to have a physical impact.

672 Mr. {Stearns.} Now, are we in the United States, you  
673 know, we have jurisdiction over energy, water, information  
674 technology, communication, nuclear plants--are we vulnerable  
675 to Stuxnet in your opinion?

676 Mr. {McGurk.} Sir, because of the ubiquitous nature of  
677 information technology in the critical infrastructure, the  
678 exploitation may occur in one sector and it could actually

679 migrate into another sector.

680 Mr. {Stearns.} So yes or no? Do you think we are  
681 vulnerable?

682 Mr. {McGurk.} I would say the vulnerabilities exist and  
683 the capability to exploit those vulnerabilities exist.

684 Mr. {Stearns.} Okay. So the big question is that the  
685 American people want to know what has the United States  
686 Government done about that to make sure we don't have that  
687 attack?

688 Mr. {McGurk.} Much of the Department's focus over the  
689 past several years has been on mitigating the vulnerabilities  
690 associated with those critical infrastructure systems.

691 Mr. {Stearns.} Do you do it by having innocuous or  
692 something that inoculates us from this software or do you do  
693 it to make sure you don't put the USB port or how are you  
694 doing this?

695 Mr. {McGurk.} So it is a multifaceted approach, sir.  
696 Much of it is through an education program, so we work with  
697 the private sector to develop standards required to educate  
698 the community on good practices and uses of equipment and  
699 technology. We actually conduct--

700 Mr. {Stearns.} You think education alone would do it?

701 Mr. {McGurk.} No, sir. We also conduct vulnerability  
702 analyses of products in our laboratories in conjunction with

703 the national laboratory community where we actually take  
704 vendors products and do a complete vulnerability assessment  
705 of those products. We also develop practices for owners and  
706 operators because in some cases, especially in the power  
707 companies, it is not a matter of replacing the technology, so  
708 you have to be able to put practices in place that mitigate  
709 the risk. And they are also working with the security  
710 communities to actually provide an enclaving capability so  
711 that we can secure the environments around which they  
712 operate.

713         So by taking this multifaceted approach, we can identify  
714 not necessarily the threat actors and focus on the threats  
715 which are coming from many areas, but the vulnerabilities  
716 themselves and mitigating the risks associated with those  
717 vulnerabilities.

718         Mr. {Stearns.} Let me ask you a question but with this  
719 Stuxnet. What have we done to protect those specific  
720 vulnerabilities in Seimens' product? In other words, has DHS  
721 issued a guidance on this?

722         Mr. {McGurk.} Yes, sir. The Department, when we  
723 started analyzing Stuxnet back in July of last year, we  
724 identified the capabilities of the particular piece of mal  
725 code. We understood its capabilities and subsequently we put  
726 mitigation plans in place working with the specific sectors

727 to identify the mitigation strategies associated with that.  
728 But since that particular piece of mal code was looking for a  
729 very unique combination of hardware and software, it was easy  
730 to identify what the mitigation strategies would be.

731 Mr. {Stearns.} Okay. Ms. Stempfley, just last Friday,  
732 the head of US-CERT resigned. US-CERT is the group charged  
733 with collaborating with state and local governments and  
734 private industry on cyber attacks. There have been a number  
735 of recent attacks on government systems, the Senate, FBI,  
736 CIA, and even a Gmail hacking aimed at top government  
737 officials. Have all of these recent attacks caused any  
738 change in the direction or change in the operation in US-  
739 CERT?

740 Ms. {Stempfley.} No, sir. The US-CERT's set of  
741 responsibilities stays the same. And as we commented in the  
742 opening statements and your opening statements as well, this  
743 is a very sophisticated environment and it is constantly  
744 evolving. And as a part of that evolution, we understand  
745 that we have to have a bench and a mechanism for growth of  
746 individuals as we go forward. And so Randy's departure was a  
747 decision that he made and we have a continued direction and  
748 focus in prevention, preparedness, and restoral  
749 responsibilities across the board.

750 Mr. {Stearns.} What were the vulnerabilities that

751 allowed these systems to be infiltrated, and do these same  
752 kind of vulnerabilities exist in the private sector and on  
753 control systems?

754 Ms. {Stempfley.} I am sorry, sir. Could you repeat the  
755 question?

756 Mr. {Stearns.} With regard to the Senate, FBI, and CIA  
757 and even the Gmail hacking aimed at top government officials,  
758 what were the vulnerabilities that allowed these systems to  
759 be infiltrated?

760 Ms. {Stempfley.} There were a number of vulnerabilities  
761 that were associated with these kinds of events that  
762 occurred, and to respond to where are other members of the  
763 private sector potentially vulnerable, I believe that is a  
764 true statement. As we commented earlier, there are a great  
765 deal of vulnerabilities that exist in the environment, and  
766 you will see that through the production of warning products  
767 and awareness notifications, we provide mitigations and  
768 indicators for private-sector owners and operators to put in  
769 place in their infrastructure. It is a shared responsibility  
770 between us and the private sector in order to implement the  
771 restorative and preventative measures.

772 Mr. {Stearns.} Thank you. My time has expired. The  
773 gentlelady from Colorado.

774 Ms. {DeGette.} Thank you very much, Mr. Chairman.

775 I want to go a little bit more in depth into some of the  
776 issues that we face trying to work on interoperability  
777 between our governmental agencies and privately owned  
778 endeavors. In particular with our communications  
779 infrastructure, which is of course an essential part of our  
780 critical infrastructure, one of the things I am concerned  
781 about 90 percent of our communications networks are privately  
782 owned by commercial carriers. So traditionally, the FCC has  
783 worked with commercial carriers to ensure the reliability of  
784 the communications networks, and under current FCC rules,  
785 carriers have to report regarding outages on legacy  
786 telecommunications system. Now, the FCC in turn uses this  
787 data to help industry standards groups to improve on the best  
788 practices.

789 So I am wondering, Ms. Stempfley and Mr. McGurk, if you  
790 can talk to me a minute given FCC's historical involvement  
791 with the communications infrastructure and the relationship  
792 with commercial carriers, don't you think that they can take  
793 an important role in helping drive greater awareness of cyber  
794 threats?

795 Ms. {Stempfley.} So reporting is always good and the  
796 ability to get information about what is going on is an  
797 important part of how we can frame that national picture of  
798 what is happening and the response activities. So we have a

799 history of working both with private industry directly and  
800 with other members of government in order to increase the  
801 awareness and the response actions that are necessary. I  
802 think the same would be true here.

803 Ms. {DeGette.} Mr. McGurk?

804 Mr. {McGurk.} In addition, ma'am, what I would like to  
805 add is that in response to the reporting that is conducted,  
806 part of the capability that exists within the NCCIC is our  
807 National Center for Coordination for Communications. And  
808 they receive those direct reports. So from a situational-  
809 awareness standpoint, the watch center receives real-time  
810 reporting from not only the telecommunication industry itself  
811 but also from other federal departments and agencies so that  
812 we get a better understanding from a holistic view on the  
813 impacts to communications because as we recognize that many  
814 of the critical infrastructures are relying on communications  
815 for controlling issues, for communications issues, and for  
816 flowing of data.

817 In addition, we have the physical carriers themselves  
818 located within the watch environment so that they can provide  
819 up-to-date and actionable intelligence so that we can take  
820 the necessary steps and make proper recommendations.

821 Ms. {DeGette.} Now, the office of Homeland Security  
822 coordinates those efforts on cyber threats. And so I guess

823 my question to you following up is if there is a breach in  
824 the communications network, then how do DHS and FCC respond?  
825 How do they interact together to respond?

826 Mr. {McGurk.} Part of the National Cyber Incident  
827 Response Plan includes the development and coordination of a  
828 cyber-unified coordination group or cyber UCG. This is a  
829 steady state body of emergency response and incident handlers  
830 at working level, at the operational level, and then also at  
831 the senior decision-making level. For our cyber UCG seniors,  
832 it encompasses individuals from the departments and agencies  
833 that are at the assistant secretarial level or higher. So  
834 these are the actual decision-makers in the Federal  
835 Government. And then we have a staff which encompasses not  
836 only private sector but representatives from the federal  
837 departments and agencies that coordinate on a daily basis and  
838 share real-time information whether it comes from the  
839 communications sector, the energy sector, or one of the other  
840 18 critical infrastructures. So that enables us to have that  
841 constant flow of data and provide that actionable  
842 intelligence so that private-sector companies can take the  
843 necessary steps to mitigate risk.

844 Ms. {DeGette.} Okay. Now, as I understand it, the FCC  
845 has proposed to rule this spring to extend reporting  
846 requirements about network shortages to the broadband network

847 and they are taking public comments on that issue. And so,  
848 Mr. Wilshusen, I was going to ask you do you think that  
849 collecting data on broadband outages would help gain a better  
850 understanding of when hackers have gotten into our systems?

851 Mr. {Wilshusen.} We haven't examined that issue, but I  
852 would imagine collecting information can only be helpful in  
853 making such a determination.

854 Ms. {DeGette.} Okay. And for the other two witnesses,  
855 do you have any thoughts on the potential for reporting  
856 broadband network outages to contribute to situational  
857 awareness like after there is a major emergency, something  
858 like that?

859 Mr. {McGurk.} Yes, ma'am. I believe as Ms. Stempfley  
860 had mentioned earlier, reporting is good and more reporting  
861 is even better. So the more information that enables us to  
862 develop that common operation picture that takes all of the  
863 data that we are receiving and then fuses that together. So  
864 the more information we receive in the NCCIC the better  
865 situational awareness we can provide not only to the  
866 secretary of Homeland Security and the other executive  
867 secretaries, but also to the President for decision-making  
868 capability.

869 Ms. {DeGette.} And just one last question relating to  
870 my opening statement about our communications networks is

871 there is a lot of issues around supply chains for equipment  
872 and components that have been manufactured abroad for use in  
873 the U.S. So I am wondering if these two witnesses on the  
874 end, Ms. Stempfley and Mr. McGurk, can talk about this  
875 publicly. Can you talk about how DHS is working with other  
876 federal agencies to address that issue of supply chain that  
877 part of it is foreign?

878 Ms. {Stempfley.} So as you pointed out, the  
879 telecommunications supply chain activities are an interagency  
880 response within the Federal Government. It would be more  
881 than happy to bring another agency body back to discuss that  
882 in detail?

883 Ms. {DeGette.} Thank you.

884 Thank you very much, Mr. Chairman.

885 Mr. {Stearns.} I thank the gentlelady.

886 The gentleman from Texas, Dr. Burgess, recognized for 5  
887 minutes.

888 Dr. {Burgess.} Thank you, Mr. Chairman.

889 Now, if I understand things correctly, there is an  
890 authority that exists within the executive branch to take  
891 some control of transmission grid operations in the event of  
892 a national emergency, is that correct? Either of DHS  
893 witnesses.

894 Mr. {McGurk.} Yes, sir. The Secretary for the

895 Department of Energy has that authority.

896 Dr. {Burgess.} And is it necessary to place any limits  
897 on that authority?

898 Mr. {McGurk.} Sir, I have the luxury of being a simple  
899 sailor and an operator and I don't normally identify or make  
900 recommendations on policy or operational requirements. I can  
901 say that within the guidelines that we currently have and the  
902 authorities that we currently have, we are able to execute  
903 our mission both efficiently and effectively. So I will  
904 leave that to other members of the Department to comment as  
905 far as additional requirements.

906 Dr. {Burgess.} Ms. Stempfley, do you have any thoughts  
907 on that?

908 Ms. {Stempfley.} Respectfully, sir, I believe that  
909 would be most appropriate for DHS not to comment on the legal  
910 authorities of another department.

911 Dr. {Burgess.} Well, let me ask you this. Should such  
912 an authority be necessary? Should such an occurrence happen  
913 that the authority was necessary? How long would you expect  
914 that presidential emergency authority to be exercised over a  
915 continuous time period?

916 Ms. {Stempfley.} Regrettably, sir, I am not in the  
917 position to answer that question.

918 Dr. {Burgess.} Well, let me ask you this. It seems

919 like--and I think it was referenced by either the chairman or  
920 the ranking member in their opening statements--is that we  
921 are hearing more and more about this. Does this just reflect  
922 the situational awareness that these types of threats and  
923 these types of attacks can occur or is, in fact, this a real  
924 phenomenon with the rapidity with which these attacks are  
925 coming is increasing?

926 Ms. {Stempfley.} So I believe it is all of those  
927 things, sir. There is certainly more awareness within the  
928 community of the importance of cybersecurity and the overall  
929 activity. That is increasing both the detection actions that  
930 are occurring and the reporting actions that exist. Based on  
931 that awareness and what we are seeing is that increase across  
932 the board.

933 We are also, as we all indicated in our opening  
934 statement, seeing an increase in sophistication of the  
935 attacks as they occurred as well. So I believe it is a  
936 phenomenon of all things, sir.

937 Dr. {Burgess.} Mr. McGurk, do you have any thoughts on  
938 that?

939 Mr. {McGurk.} Not in addition, sir. The only thing I  
940 would add was that because of the adoption of information  
941 technology capabilities into the critical infrastructure, we  
942 are also exposing a greater landscape of vulnerabilities to

943 areas that were in the past specifically closed off and  
944 proprietary in nature. So by adopting that technology, we  
945 also advance the vulnerability landscape associated with  
946 those critical infrastructure operations.

947 Dr. {Burgess.} Well, one of the hazards in this is you  
948 are always fighting the last attack. What sort of forward-  
949 looking policies and procedures are being implemented by DHS?  
950 Are you looking into for wherever the perpetrator is, what is  
951 the value that they are deriving from these and are there  
952 ways that we can perhaps preempt some of these attacks before  
953 they happen rather than just simply reacting to them?

954 Mr. {McGurk.} Sir, part of what the National Cyber  
955 Incident Response Plan focuses on is moving from the left end  
956 of the continuum where we are primarily focusing on response  
957 and recovery, which to your point, sir, is accurate. We are  
958 always fighting that last event or that last battle.

959 What we are looking forward to working with the private  
960 sector is moving to the right and putting the preparedness,  
961 the protective, and the preventative measures in place. And  
962 we are taking, again, a multifaceted approach through  
963 advanced technology, working with the owners and operators,  
964 and also with the vendor community to establish criteria for  
965 new systems and new operational parameters.

966 The Department produces a procurement guideline for

967 owners and operators which talks about security requirements  
968 for new systems and new operating procedures. And we also  
969 work closely with the integration community so that we are  
970 identifying how to install and how to manage these systems as  
971 they are being updated in the critical infrastructure. So we  
972 are looking at it as a continuum shifting more from the left,  
973 the responsive part, over to the right where we are being  
974 preventative and predictive.

975 Dr. {Burgess.} Now, a vast majority of this critical  
976 infrastructure is in private hands, is that correct?

977 Mr. {McGurk.} That is correct, sir.

978 Dr. {Burgess.} So is there any type of analysis as to  
979 the cost that may be incurred by the private sector to keep  
980 up with what you just articulated.

981 Mr. {McGurk.} Yes, sir. In fact, the Department  
982 identifies and describes risk as an equation of threats,  
983 vulnerabilities, and consequences. When we work with the  
984 private sector, we understand that the denominator there is  
985 also cost. So the procurement standards that I had mentioned  
986 earlier takes that into account. Not everything can be a  
987 gold standard. We are not saying that you have to have  
988 absolute security across the board. It is a risk-based  
989 approach so we take that same levelized approach and build  
990 the business case to identify what we need to implement in

991 what areas. So if we are going to spend a dollar to mitigate  
992 risk, should we focus on the threats or should we focus on  
993 mitigating the risks and the vulnerabilities? And then what  
994 are the subsequent consequences associated with that? That  
995 is really one of the approaches that we are taking in  
996 addressing this issue.

997 Dr. {Burgess.} And do you solicit and accept input from  
998 the private sector, the owners of the critical infrastructure  
999 as to that pricing consideration?

1000 Mr. {McGurk.} Yes, sir. In fact, as the chairman had  
1001 mentioned earlier, one of the things that we focus on is a  
1002 number of working groups. And in the industrial control  
1003 systems area, we actually sponsor a joint public-private  
1004 working group, the Industrial Controls System Joint Working  
1005 Group, ICSJWG, which looks at not only mitigating risks but  
1006 also product development, implementation, education, and a  
1007 whole host of issues. And that is a complete joint  
1008 environment with both public and private members represented.

1009 Dr. {Burgess.} Thank you, Mr. Chairman. I will yield  
1010 back.

1011 Mr. {Stearns.} I thank the gentleman.

1012 Dr. Christensen is recognized for 5 minutes.

1013 Dr. {Christensen.} Thank you, Mr. Chairman.

1014 Again, welcome to our panel.

1015 Under Homeland Security Presidential Directive 7,  
1016 healthcare and public health are identified as critical  
1017 infrastructure sectors, and of course the healthcare sector  
1018 plays a significant role in response and recovery in the  
1019 event of a disaster. So I would like to talk with all of our  
1020 witnesses about the efforts to protect this sector against  
1021 cyber threats.

1022 Beginning with Ms. Stempfley and Mr. McGurk, what do you  
1023 see as the major challenges to ensuring cybersecurity in the  
1024 healthcare sector?

1025 Ms. {Stempfley.} Ma'am, I will begin with some of the  
1026 kinds of policy challenges we have been working through in  
1027 the Federal Government associated with this. And so, for  
1028 example, we are working to deploy technological solutions  
1029 that enable detection and prevention measures in place.  
1030 Those technological solutions oftentimes require a very  
1031 detailed analysis of the kinds of privacy and protection  
1032 requirements that need to be put in place that we all feel so  
1033 strongly about as well and we need to work through some of  
1034 those key policy nexuses between the two so that we can  
1035 provide that kind of support and prevention support while  
1036 still being very true to the protection measures that we feel  
1037 so strongly about in terms of privacy and other areas.

1038 Those kinds of infrastructure systems are very important

1039 to us and we agree with that. Once we get past the policy  
1040 questions, it is a matter of how we employ those solutions,  
1041 best practices across the board and handle the equally  
1042 important integrative systems that exist in healthcare and  
1043 have that nexus between IT and embedded systems as well.

1044 Mr. {McGurk.} Yes, ma'am. I would also mention that  
1045 one of the Department's focuses is also on not just  
1046 protecting the information in accordance with a number of  
1047 regulations and requirements but also the equipment itself.  
1048 When we look at the vulnerabilities associated with the other  
1049 sectors, the healthcare industry also has an equal number of  
1050 vulnerabilities associated with embedded medical devices or  
1051 with advanced technology that could potentially be exploited  
1052 because of the inherent communications capability of those  
1053 devices.

1054 So again, the Department is taking not just a data-in-  
1055 motion, data-at-rest approach, but a holistic approach to the  
1056 healthcare industry, working with the private sector, working  
1057 with the manufacturers of these pieces of equipment, and also  
1058 with the necessarily federal departments and agencies so that  
1059 we understand the risks associated with healthcare industry  
1060 and provide actionable steps that will better improve not  
1061 only the quality of service but the quality of life.

1062 Dr. {Christensen.} Thank you. And those focuses

1063 estimates are great. I am assuming you are working with the  
1064 Department of Health and Human Services as well as with the  
1065 private sector.

1066 Ms. {Stempfley.} With any of the particular sectors,  
1067 ma'am, we work very strongly with the sector-specific agency  
1068 in helping Human Services specifically in the situation.

1069 Mr. {McGurk.} In fact, ma'am, we have the National  
1070 Health Information Sharing and Analysis Center coming to  
1071 visit and tour the NCCIC tomorrow and part of our development  
1072 process to get them physically located on board. So they  
1073 will be actually visiting us tomorrow so that we can identify  
1074 those connections.

1075 Dr. {Christensen.} Great. Great.

1076 Mr. Wilshusen, I am also interested in hearing more  
1077 about GAO's work on cybersecurity issues that affect health  
1078 and public health. As providers use more computer-based  
1079 mechanisms and programs to help them treat patients, and I  
1080 guess this sort of follows up on what you were saying, Mr.  
1081 McGurk, do you agree that it poses additional risk to the  
1082 personal health information could be released to the public?

1083 Mr. {Wilshusen.} Certainly. In fact, we have a couple  
1084 of engagements that we have ongoing or will start soon. One  
1085 was mandated by the High-Tech Act in which GAO is responsible  
1086 for reviewing the security and privacy protections over

1087 information that is transferred and exchanged through the  
1088 Electronic Prescription System or E-Prescribing.

1089 Dr. {Christensen.} Um-hum.

1090 Mr. {Wilshusen.} We anticipate starting that engagement  
1091 in September with the report release date on September 2012.

1092 In addition, we have another engagement that we are  
1093 currently working on to look at the security controls and  
1094 risks associated with embedded or implantable medical devices  
1095 such as insulin pumps, pacemakers and that that can be  
1096 accessed through wireless technologies and may have chips in  
1097 place. So we are also examining the report of security risk  
1098 associated with that, as well as FDA's premarket and post-  
1099 market review processes to address those particular risks.

1100 Dr. {Christensen.} Well, thank you. My time is running  
1101 out. I appreciate the information because the ever-  
1102 increasing use of technology in our healthcare system  
1103 obviously holds a lot of promise and many benefits. But also  
1104 as we increase our reliance on technology, there is also--as  
1105 you have pointed out very clearly--the opportunity to hack in  
1106 and interfere with that.

1107 So thank you, Mr. Chairman. I am out of time.

1108 Mr. {Stearns.} I thank the gentlelady. Gentlelady from  
1109 Tennessee, Mrs. Blackburn, recognized for 5 minutes.

1110 Mrs. {Blackburn.} Thank you, Mr. Chairman.

1111 Ms. Stempfley, I wanted to come with you. I was just  
1112 meeting with one of my airports, and I wanted to know--TSA.  
1113 What does the DHS and TSA do with the body images that they  
1114 collect from the scanners at the airports? How long are they  
1115 stored and do you protect these images? Do you share them  
1116 with any other agency? And what action would you take in  
1117 case you had a breach?

1118 Ms. {Stempfley.} Ma'am, the Office of Cybersecurity and  
1119 Communications is responsible for setting standards that the  
1120 Federal Government has to comply with to include TSA. I am  
1121 not familiar with their specific--

1122 Mrs. {Blackburn.} Would you get back to me on this?

1123 Ms. {Stempfley.} I certainly would.

1124 Mrs. {Blackburn.} Okay. I know that it is a part of  
1125 what we are talking about and it also pertains to the privacy  
1126 work that we are doing in our CMT Committee. And I think as  
1127 we work with some of the issues we are having with TSA, I  
1128 would love to have the answer if you could do that.

1129 I have got another question. This would be for you and  
1130 Mr. McGurk. And I mentioned TVA in my opening comments and  
1131 the amount of coverage that we have with the power security.  
1132 I want to see what your interface is with the state and local  
1133 governments and the infrastructure by facilitating the  
1134 information sharing of the cyber threats and the incidents

1135 and through the ISACs. So there are 16 of those ISACs,  
1136 right? Okay. And very briefly if you would just go through  
1137 how it works, what kind of information that is shared, what  
1138 is your process how you protect the data that you get and  
1139 what your expectation is, the state and local governments,  
1140 that they are going to protect that data and then what your  
1141 response would be if you had a breach?

1142         Mr. {McGurk.} Thank you, ma'am. I would just like to  
1143 start off by saying that we have a very close working  
1144 relationship with the Tennessee Valley Authority. In fact,  
1145 we visited many times and we share real-time information  
1146 through a number of sensor programs that we operate so that  
1147 we have a better understanding of the actual threats and  
1148 impacts and associated with those operational environments.

1149         What we do and how we share that information from the  
1150 standpoint at the national level is much of the data that is  
1151 voluntarily submitted through the NCCIC comes from either the  
1152 ISACs themselves--the Information Sharing and Analysis  
1153 Centers, including the Multi-State--or it comes from the  
1154 private-sector companies themselves. Much of that data is  
1155 submitted under the secretary's authority for the protection  
1156 of critical infrastructure information or PCII. That  
1157 protects that information from being released even to a  
1158 regulator, for instance if it is a power company and they

1159 submit the information to us.

1160 We then take that and we work directly with that company  
1161 to develop a mitigation strategy that is a) company-specific  
1162 and then b) we anonymize it to the point where it becomes a  
1163 sector-specific mitigation strategy. The RSA data breach was  
1164 a great example of how, within a short period of time, less  
1165 than 24 hours of notification of the breach, we had more than  
1166 50 companies and federal departments and agencies represented  
1167 under the Cyber Unified Coordination Group developing sector-  
1168 specific mitigation plans. So those individuals--not only  
1169 from a physical environment but also a data-sharing  
1170 environment--collaborate to generate those mitigation plans.

1171 Mrs. {Blackburn.} Okay. And at what point do you pull  
1172 state or local government into that to participate?

1173 Mr. {McGurk.} Continuously. So they actually have a  
1174 representative on the floor of the Multi-State ISAC.

1175 Mrs. {Blackburn.} Okay. Okay.

1176 Mr. {McGurk.} So they are there in real time.

1177 Mrs. {Blackburn.} All right.

1178 Ms. {Stempfley.} And ma'am, to continue on in that  
1179 discussion, we have worked with the 50 states to provide  
1180 clearances to the chief security officers in each of the  
1181 states and then share classified information through their  
1182 fusion centers so that that provides not just their

1183 representation on floor in real time around an event but also  
1184 gives us an ability post-date it to them in their states as  
1185 well.

1186 Mrs. {Blackburn.} And then do you do any coeducation  
1187 and training with local law enforcement back into your  
1188 protocols?

1189 Ms. {Stempfley.} The training activity that we provide-  
1190 -all of our training is provided on an open basis so that  
1191 state representatives can come and participate. I can't  
1192 speak to which states have chosen to come in with particular  
1193 law enforcement individuals, but we make it available to them  
1194 in order for them to take it up.

1195 Mrs. {Blackburn.} Excellent. Thank you, Mr. Chairman.  
1196 Yield back.

1197 Mr. {Stearns.} The gentlelady from Florida, Ms. Castor,  
1198 is recognized for 5 minutes.

1199 Ms. {Castor.} Thank you, Mr. Chairman. Thank you to  
1200 the witnesses for your insight today.

1201 It is apparent that an effective partnership between the  
1202 Federal Government and the private sector is necessary to  
1203 ensure the security of all of our networks, whether those  
1204 networks manage critical infrastructure or simply handle the  
1205 day-to-day data of the Federal Government and communications.

1206 Mr. Wilshusen, in your testimony you noted that the

1207 private sector has expressed concerns that DHS is not meeting  
1208 their expectations in terms of information sharing. What  
1209 concerns does private industry have about DHS' willingness to  
1210 provide information?

1211 Mr. {Wilshusen.} Yes, ma'am. We did a review in which  
1212 we surveyed 56 individuals from the private sector from five  
1213 private-sector councils. And we found that they identified a  
1214 number of key activities that they thought were critical or  
1215 important for the public-private partnership to include the  
1216 provision of timely and actionable threat and alert  
1217 information, having a secure mechanism for collecting  
1218 information or sharing information with the public sector.  
1219 And they indicated only 27 percent of those respondents  
1220 indicated that they felt that their public-sector partners  
1221 were actually meeting those expectations to a great or  
1222 moderate extent. And so there are a number of concerns about  
1223 being able, on the part of the private sector, to collect  
1224 timely information from the public-sector partners.

1225 Ms. {Castor.} Were there any particular sectors that  
1226 stood out that appeared to be problematic?

1227 Mr. {Wilshusen.} Well, from the private-sector side, it  
1228 was pretty much across the board. The five sectors that were  
1229 included in our study included the banking and finance  
1230 sector, the IT sector, the communications, energy, and the

1231 defense industrial base sectors. And it was pretty much  
1232 across the board. As I mentioned, only 27 percent out of the  
1233 56 respondents actually felt that they were receiving support  
1234 to a great or moderate extent.

1235 Ms. {Castor.} So Mr. McGurk, what is DHS doing to  
1236 address these concerns and to ensure that you all are working  
1237 collaboratively with the private sector?

1238 Mr. {McGurk.} Ma'am, I would like to start off by  
1239 saying, you know, can we do better? Absolutely. We have  
1240 modified much of the structures by actually standing up and  
1241 creating the NCCIC that met some of the requirements moving  
1242 forward, by actually having the private sector participate  
1243 and not only receiving the information but developing the  
1244 information. By having them physically present in the  
1245 environment really assists us in putting the information in a  
1246 language that is necessary to reach our constituents.

1247 A great example is in the past when we would produce  
1248 information, we would produce it in a language that we  
1249 understood, and then we would send that out and that may or  
1250 may not meet the needs of our private-sector partners. By  
1251 having power engineers and financial services specialists and  
1252 IT specialists physically sitting there working with us and  
1253 collaboratively developing the knowledge necessary to  
1254 distribute, we are able to provide actionable intelligence.

1255           Just last year we received a report in an intelligence  
1256 communication of a particularly malicious piece of mal code  
1257 that had a subject line on an email called ``here you have.``  
1258 Within a few hours of that appearing in a classified report,  
1259 the US-CERT produced an early warning and notice that went  
1260 out to the broad private sector because we took that data,  
1261 declassified it, and provided actionable intelligence for our  
1262 private-sector partners. But by having them there and  
1263 participating really enables us to provide better products  
1264 for our partners and also speeds up the time necessary to  
1265 generate that product.

1266           Ms. {Castor.} Well, how about the flip side? I am also  
1267 curious about how well the private sector is communicating  
1268 with DHS when they suffer a cyber attack or a breach, Mr.  
1269 McGurk, are private companies required to report cyber  
1270 attacks or coordinate their responses to those attacks with  
1271 DHS?

1272           Mr. {McGurk.} So there is no requirement to report the  
1273 information directly to the Department, but I think what has  
1274 happened over the development of the partnership over the  
1275 past several years is the stigma associated with cyber  
1276 breaches has started to be removed and companies are  
1277 volunteering the information because they understand that it  
1278 not only benefits their ability to maintain goods and

1279 services but it will also assist the broader community  
1280 because they recognize that when they share with the  
1281 Department, we are not going to publish company-specific  
1282 information. We are going to anonymize that and produce  
1283 mitigation strategies and plans that help the broad sectors.  
1284 And they have been working very closely with us in developing  
1285 that.

1286 Ms. {Castor.} Are there instances where DHS has become  
1287 aware of a cyber attack or a breach in a particular company  
1288 and then you contacted that company to assist and they  
1289 declined your offers to work with them, declined assistance?

1290 Mr. {McGurk.} Yes, ma'am.

1291 Ms. {Castor.} What can we do about that? How do we  
1292 improve the collaboration in working together?

1293 Mr. {McGurk.} Part of that is an awareness and an  
1294 understanding. From the private-sector standpoint, I  
1295 understand that we have to demonstrate value and they have to  
1296 see how working with DHS and partnering with DHS adds value  
1297 to their capability. In some cases, those particular  
1298 companies had a very advanced capability. We gave them the  
1299 early-warning notice that they needed to take the necessary  
1300 steps to protect their networks. So subsequently, additional  
1301 response from DHS wasn't required. And in the extreme case,  
1302 we received declination for support but recognition of the

1303 awareness or the alert.

1304 Ms. {Castor.} Thank you very much.

1305 Mr. {McGurk.} Thank you, ma'am.

1306 Mr. {Stearns.} The gentleman from Virginia is  
1307 recognized for 5 minutes, Mr. Griffith.

1308 Mr. {Griffith.} I am just curious, Mr. McGurk, under  
1309 what circumstances, if any, would the DHS NCCIC withhold  
1310 cyber threat information that it has encountered from owners  
1311 or operators of critical infrastructure?

1312 Mr. {McGurk.} Sir, we do not withhold threat  
1313 information, but subsequently, we don't develop threat  
1314 information. Under the authorities of the Department, we  
1315 focus primarily on mitigation of risk, and that is where we  
1316 focus our activities. Threat information is really developed  
1317 by the intelligence community and we rely on that partnership  
1318 with the intelligence community to identify threat actors.

1319 Mr. {Griffith.} All right. Do you have any indication  
1320 that they may be sometimes withholding information?

1321 Mr. {McGurk.} No, sir. In many cases, what is germane  
1322 to mitigation is not necessarily associated with the actor.  
1323 It is the activity. So it is the exploitation of the  
1324 vulnerability which is necessary to share to protect the  
1325 networks, not who is actually doing it.

1326 Mr. {Griffith.} Mr. Wilshusen, the GAO reported in

1327 October of 2010 that only 2 of 24 recommendations by the  
1328 President Cybersecurity Policy Review had been implemented  
1329 and the rest had only been partially implemented. What can  
1330 you tell us about whether any additional progress has been  
1331 made?

1332 Mr. {Wilshusen.} Well, one of the reasons we found that  
1333 the partial implementation occurred was because many of the  
1334 agencies were not taking effect because they were not given  
1335 specific roles and responsibilities to implement some of  
1336 those recommendations, and that kind of delayed actions to  
1337 implementing that. We will be following up as part of our  
1338 annual review follow-up on our recommendations to see what  
1339 extent those recommendations are now being met. But since we  
1340 just issued that in October, we have not gone back to follow  
1341 up on our prior recommendations and to do a reassessment.

1342 Mr. {Griffith.} Should we expect an updated report this  
1343 coming October?

1344 Mr. {Wilshusen.} We will be updating the status of our  
1345 recommendations, and if you request us to do it, we will  
1346 certainly do it.

1347 Mr. {Griffith.} I would be curious since only 2 of the  
1348 24--

1349 Mr. {Wilshusen.} Right.

1350 Mr. {Griffith.} --were implemented as of last year, and

1351 I am just wondering should we be concerned that so few of the  
1352 recommendations had been fully implemented at that time?

1353 Mr. {Wilshusen.} Well, there are 10 near-term  
1354 recommendations coming out of that policy review, 14 mid-term  
1355 recommendations. Several of the mid-term recommendations are  
1356 actions of such a nature that it is going to take multiple  
1357 years to fully implement those. But the near-term  
1358 recommendations are very important and they should be  
1359 implemented as soon as possible.

1360 Mr. {Griffith.} All right. I thank you. Yield back my  
1361 time.

1362 Mr. {Stearns.} The gentleman yields back.

1363 Yes?

1364 Dr. {Burgess.} Would you yield to me for follow-up  
1365 questions?

1366 Mr. {Griffith.} I yield for follow-up.

1367 Dr. {Burgess.} Dr. Christensen asked some very good  
1368 questions on the healthcare aspects of the critical  
1369 infrastructure and going along with what the gentleman was  
1370 just asking as far as those forward-looking threats, it seems  
1371 like we have created some problems for ourselves in the High-  
1372 Tech Act and some of the things we have done with the  
1373 information technology infrastructure as applied to health.  
1374 Star Clause, for example, which prohibit hospitals from

1375 putting wire in a doctor's office if the doctor is not  
1376 directly affiliated with the hospital. So pushing a lot of  
1377 these vertically integrated systems to go on the internet in  
1378 order to have the abilities or the ease of transfer of the  
1379 data, which then renders them vulnerable to attacks on the  
1380 internet. Have you looked at that, whether perhaps there is  
1381 something that could be done on the policy side to lessen the  
1382 impact of the vulnerability if we were to make some changes  
1383 on the regulatory side? A closed loop if you would between  
1384 the hospital and a group of doctors, even though they are not  
1385 all part of the same business model might be one way to do  
1386 that. Have you explored that at all?

1387 Ms. {Stempfley.} So your example is a wonderful example  
1388 of furthering the independence between the infrastructures as  
1389 they go forward.

1390 Dr. {Burgess.} No, it is an example of how we make  
1391 things harder than they need to be in the first place and  
1392 then we have got to do a whole bunch more stuff to make it  
1393 workable in the real world. But continue.

1394 Ms. {Stempfley.} Thank you, sir. The specific reviews,  
1395 technical reviews of proposals is not something that we  
1396 certainly do. What we work towards are best practices for  
1397 the kinds of separation and containment that might be  
1398 necessary in order to understand the environment. Each of

1399 the owners and operators has a better understanding of the  
1400 risks in their particular environment in the business models  
1401 that best serve them in each of these cases. And so the set  
1402 of best practices are an important part of how we do this.

1403 Dr. {Burgess.} But do we look at the regulations that  
1404 we, the Federal Government, have put in place that make it  
1405 harder for people to do the right thing in the real world?

1406 Ms. {Stempfley.} So I am not sure I can say that  
1407 specific regulation was reviewed prior to in order to  
1408 understand the potential implications across the board, but  
1409 we do look at regulations and procedures as they come up.

1410 Dr. {Burgess.} I appreciate the gentleman for yielding.  
1411 My time has expired. Let us look at that going forward. I  
1412 yield back.

1413 Mr. {Stearns.} I thank the gentleman.

1414 Ms. Schakowsky is recognized for 5 minutes.

1415 Ms. {Schakowsky.} Thank you.

1416 Have any of you, the three of you, read Stieg Larsson's  
1417 book, the Girl with the Dragon Tattoo, et cetera?

1418 Mr. {Wilshusen.} Yes.

1419 Ms. {Schakowsky.} You have. If you haven't, people who  
1420 are into cybersecurity would not only enjoy them but probably  
1421 be a little worried about it. The pretty flawed heroine,  
1422 Lisbeth Salander, there is no firewall too high or wide or

1423 low that she can't get through. And I think she is the  
1424 heroine, sort of the good guy, but the notion of individual  
1425 actors out there who have this tremendous capacity to  
1426 infiltrate I think is a real concern. I sit also on the  
1427 Intelligence Committee, and we think about that a lot.

1428         So here is what I wanted to ask. Do we employ sort of  
1429 old-school kinds of techniques like redundancy to make sure--  
1430 I remember sitting in a hotel room watching a rolling  
1431 blackout in Ohio a number of years ago, which turned out to  
1432 be a failure of the grid and not some sort of attack--this  
1433 was post-9/11--but felt like it might have been. So do we  
1434 build in things like we do in aircraft or whatever, just  
1435 redundancies so we are not as vulnerable? Can someone  
1436 answer?

1437         Mr. {McGurk.} Yes, ma'am. I do agree that one of the  
1438 salient points of the book was that they were focusing on  
1439 perimeter defense as a method of ensuring their security, and  
1440 as you quite adequately pointed out that there was no wall  
1441 too high or too thick that she couldn't get through in the  
1442 process, and subsequently, that is why the Department doesn't  
1443 look at only a perimeter-defense strategy as part of enabling  
1444 a sound cybersecurity profile. We look at a defense-in-depth  
1445 strategy so that there is layers upon layers of security  
1446 implemented. In addition, we want to focus on the practices

1447 and procedures to address the various risk associated with  
1448 operating those networks. Whether it is from insider  
1449 activity, whether it is from nation-state-sponsored, whether  
1450 it is criminal activity, we treat the act separate from the  
1451 actors so that we can understand what they are trying to  
1452 exploit as far as the vulnerabilities. So that is the  
1453 approach that the Department takes, and we do work very  
1454 closely with the intelligence community, law enforcement  
1455 community, and the private sector to develop those necessary  
1456 strategies so that we can have a better and more secure  
1457 defense posture.

1458       Ms. {Schakowsky.} Let me ask another question. There  
1459 is a lot of talk and even advertising about how we can  
1460 centralize data management and storage and concentration and  
1461 that you can access that without individual servers and all  
1462 kinds of things to make business more efficient, et cetera.  
1463 I am wondering if this creates a new layer, then, of  
1464 vulnerability if everything is sort of outsourced to one  
1465 place.

1466       Ms. {Stempfley.} The what I call re-architecting  
1467 moments that are going on in the environment, things like the  
1468 movement to cloud computing and mobility are intelligent and  
1469 opportunity at the same time. So there certainly are  
1470 vulnerabilities that exist in that environment that must be

1471 addressed as we architect to move things there. But it isn't  
1472 generally a lump sum, just pick up and move. There are  
1473 design considerations that must be taken into account as you  
1474 move. And so they are these opportunities for individuals to  
1475 look at how they both handle their data procedurally and how  
1476 they protect it through this defense-in-depth approach across  
1477 the board.

1478       Mr. {Wilshusen.} And if I may add we did a review over  
1479 the clouds computing security and identified a number of both  
1480 positive as well as negative security implications of going  
1481 to the cloud computing. Particularly of the negative sort is  
1482 just agencies lose control over the access to their data, who  
1483 has access to it, as well as the ability of agencies who are  
1484 still responsible for the protection of that information to  
1485 assure themselves through independent testing or other  
1486 evaluations that the cloud service provider is actually  
1487 implementing security effectively over their environment and  
1488 the information. And those are still issues that are still  
1489 being worked out. The Federal Government, through GSA--I am  
1490 not sure if DHS is involved in this--OMB and others are  
1491 studying up different procedures through FedRAMP and some  
1492 other programs to try to address some of those areas.

1493       Ms. {Schakowsky.} I started by talking about this  
1494 rolling blackout that I saw. I wondered if we can talk about

1495 how secure our power grid really is. I don't know if you  
1496 addressed that earlier. There was a project that showed the  
1497 effect of hacking into a power plant's control station via  
1498 computers and digital devices, so I am just wondering how  
1499 that came out and if there are vulnerabilities that we are  
1500 correcting?

1501 Mr. {McGurk.} Yes, ma'am. The purpose behind the  
1502 Aurora evaluation and experiment that was conducted by the  
1503 Department in conjunction with the Idaho National Lab back in  
1504 2007 was essentially identifying the interdependencies  
1505 between the critical infrastructures. That is how it started  
1506 out. We wanted to see if we could have a negative impact in  
1507 an environment by attacking the capabilities or the equipment  
1508 of another environment. For instance, if I destroyed the  
1509 generation capability, could I then have an adverse impact on  
1510 a data-storage center or an airport or some other physical  
1511 infrastructure? So subsequently, we took a look at the  
1512 interconnected nature of these devices and we conducted a  
1513 series of experiments that identified the capability by  
1514 modifying settings and accessing control networks to actually  
1515 take a digital protective circuit and turn it into a digital  
1516 destructive circuit.

1517 A simple explanation of what we did with Aurora it is  
1518 like you are driving down the road at 60 miles an hour and

1519 you throw your transmission in reverse, it is going to have a  
1520 negative impact on that car to operate.

1521 Ms. {Schakowsky.} Yeah.

1522 Mr. {McGurk.} So that is really what we were trying to  
1523 demonstrate. And then subsequently, once we identify the  
1524 vulnerabilities, how do we put those protective measures in  
1525 place, whether it is through equipment design and  
1526 modification or in many cases it is just through procedural  
1527 changes? So we look at low-cost or no-cost approach. From  
1528 that point forward, the Department has conducted numerous  
1529 equipment vulnerability assessments to not only identify  
1530 inherent vulnerabilities in devices but to work with industry  
1531 to develop those mitigation strategies and in some cases  
1532 working with the manufacturers to physically modify the  
1533 equipment so it is more secure.

1534 Ms. {Schakowsky.} Thank you. My time has well expired.  
1535 Thank you.

1536 Mr. {Stearns.} The gentleman from Louisiana, Mr.  
1537 Scalise, recognized for 5 minutes.

1538 Mr. {Scalise.} Thank you, Mr. Chairman. If I could ask  
1539 all the panelists first, I just want to get your opinion on  
1540 if our critical networks are more vulnerable today than they  
1541 were 5 years ago?

1542 Ms. {Stempfley.} So my opinion is they are not

1543 necessarily more vulnerable than they were 5 years ago. A  
1544 great deal has happened over the last 5 years in terms of  
1545 coordination, collaboration across the board. What I believe  
1546 is that we are much more aware now than we were 5 years ago  
1547 both of the role that they play in the environment. We are  
1548 certainly more dependent on cybersecurity solutions and  
1549 interdependent today, more aware of that, and there is a  
1550 higher sophistication in the threat that exists today than  
1551 did some time ago.

1552 Mr. {Scalise.} Mr. McGurk?

1553 Mr. {McGurk.} Thank you, sir. I would also agree that  
1554 I believe it has been an evolutionary period. Perhaps in the  
1555 past we were focusing more on information assurance as a  
1556 method of achieving cybersecurity, but since then, we have  
1557 recognized that since the physical and the virtual are all  
1558 interconnected, we are taking a more direct approach towards  
1559 cybersecurity. So there may be more reporting but there is  
1560 more awareness as well.

1561 Mr. {Wilshusen.} And I would also say that the threats  
1562 to cyber critical infrastructures are increasing. They are  
1563 evolving and growing and becoming more sophisticated. So  
1564 those two raise the overall risk to those infrastructures.  
1565 Our reviews have shown that where we have evaluated the  
1566 security over specific systems that they are vulnerable and

1567 that numerous vulnerabilities exist because appropriate  
1568 information security controls, which are well known, have not  
1569 been implemented on a consistent basis throughout. So while  
1570 there is greater awareness, there is also a greater threat I  
1571 believe and also the vulnerabilities still remain.

1572 Mr. {Scalise.} Mr. Wilshusen, in your testimony, the  
1573 GAO--and you listed here some GAO recommendations to enhance  
1574 the protection of cyber-reliant critical infrastructure.  
1575 Regarding these recommendations that you laid out, do you see  
1576 that other agencies are looking at these or open to these and  
1577 specifically with members of DHS that are here and, you know,  
1578 I would like to get their take, too, but what has been the  
1579 reaction you have seen from the GAO report of these specific  
1580 recommendations?

1581 Mr. {Wilshusen.} Well, for most of our reports in this  
1582 area, we have received largely concurrences with our  
1583 recommendations, particularly from DHS. They have taken a  
1584 number of actions to implement our recommendations and we  
1585 will be following up with them to ensure that they are  
1586 effectively implemented over time. In some cases, even when  
1587 DHS non-concurred for the purposes of our report with the  
1588 recommendation, they ultimately reversed themselves and  
1589 decided to implement the recommendations. So I think there  
1590 is awareness and concurrence for the most part of the

1591 agencies to implement our recommendations.

1592 Mr. {Scalise.} I will ask the same, Mr. McGurk and Ms.  
1593 Stempfley, just both of those recommendations but also other  
1594 tools that you think should be available.

1595 Mr. {McGurk.} I would like to add that in addition to  
1596 the recommendations of GAO--and we do evaluate them not only  
1597 from a technical standpoint but also from an implementation  
1598 standpoint, and that is part of the challenge that we  
1599 identified. In the critical infrastructure, the networks are  
1600 so--in some cases--unique that you can't apply a particular  
1601 standard or requirement that is identified by a  
1602 recommendation and you may actually cause an interoperability  
1603 challenge. So we do look at that from a technical standpoint  
1604 and then we work with other standards-settings bodies such as  
1605 NIST to identify those best practices and those requirements  
1606 and then work with the private sector to ensure that we can  
1607 actually implement that without causing an adverse impact or  
1608 additional cost.

1609 Mr. {Scalise.} Ms. Stempfley?

1610 Ms. {Stempfley.} So we agree that the recommendations  
1611 in the GAO report are ones that we focus a great deal of  
1612 attention on and recognize that cyber is one of the high-risk  
1613 items that GAO executes. We have a regular interaction with  
1614 them around this particular activity, particularly given the

1615 consequences. We talked a great deal about consequences of  
1616 malicious activity in this particular environment. We watch  
1617 very closely that. And as we work through issues both in  
1618 terms of owners and operators, execution and implementation  
1619 of practices in their environment and come out as we are  
1620 requested to come out and provide voluntary review of  
1621 information and infrastructures and the owner/operators we  
1622 are also able to identify how they are doing in terms of  
1623 implementation and get information about what is generally  
1624 accepted practices across the board.

1625       Mr. {Scalise.} Real quickly one final question before  
1626 my time runs out. The Department of Defense's director of  
1627 intelligence and counterintelligence has talked about supply  
1628 chain integrity and, you know, they suggest that some  
1629 equipment that we buy, hardware that we buy could be  
1630 corrupted both hardware and software. And there are some  
1631 things that they are looking at in that regard, and I wanted  
1632 to get your take from Homeland Security or if GAO wants to  
1633 chime in. Is that something that you all have looked at as  
1634 well? Have you seen any problems there?

1635       Ms. {Stempfley.} So I believe I made an offer earlier  
1636 to bring back an interagency review around supply chain. We  
1637 appreciate that it is important for us to look across the  
1638 entire lifecycle of both equipment and of software

1639 development as well so that we can make sure that we have  
1640 good practices in each of the steps of the lifecycle.

1641 Mr. {Wilshusen.} And if I may chime in, we are  
1642 currently evaluating the supply chain risk process at several  
1643 agencies including DOD, DHS, Justice, Energy as part of our  
1644 review over the supply chain risks for IT. We are assessing  
1645 also the agencies' efforts to employ a risk-based approach to  
1646 assessing supply chain risks.

1647 Mr. {Scalise.} Thank you, Mr. Chairman. I yield back.

1648 Mr. {Stearns.} Thank you.

1649 The gentleman from Texas, Mr. Green, is recognized for 5  
1650 minutes.

1651 Mr. {Green.} Thank you, Mr. Chairman.

1652 And following up our colleague from Tennessee, Ms.  
1653 Blackburn, you know, our committee has jurisdiction both over  
1654 cybersecurity and healthcare, and so when we go through those  
1655 screenings, could we at least maybe in our jurisdiction have  
1656 a radiologist look at those so we can do those full body  
1657 scans and it maybe save us on our imaging cost.

1658 But I want to welcome our panel here. It has been a  
1659 long hearing for you all and I thought we ought to laugh a  
1660 little bit.

1661 The GAO has long identified protecting the Federal  
1662 Government's information system and Nation's cyber-critical

1663 structures. And Mr. Wilshusen, when did the GAO first  
1664 identify cybersecurity as part of our high-risk series?

1665 Mr. {Wilshusen.} That was back in 2003.

1666 Mr. {Green.} Okay. And you did your first major review  
1667 of DHS cybersecurity efforts in 2005?

1668 Mr. {Wilshusen.} That is right. That is when we  
1669 assessed the Department's performance and actually  
1670 implementing some 13 roles and responsibilities that it was  
1671 responsible for.

1672 Mr. {Green.} Have you seen improvements in the way that  
1673 the Federal Government prepares for and addresses cyber  
1674 threats since you have been reviewing DHS' program?

1675 Mr. {Wilshusen.} We have seen progress at DHS in the  
1676 way that it is addressing some of these areas. We also  
1677 recognize that there is more that needs to be done,  
1678 particularly with some of the sector's specific planning  
1679 efforts, its cyber analysis and warning capabilities, as well  
1680 as just as I mentioned earlier related to its private-public  
1681 partnerships.

1682 Mr. {Green.} Okay. I understand in 2009 DHS launched  
1683 the 24-hour DHS-led coordinated watch and warning system  
1684 known as the National Cybersecurity Communications  
1685 Integrations System. Mr. McGurk, what private-sector  
1686 entities have current access to the resources of this

1687 facility?

1688           Mr. {McGurk.} Certainly, sir. Currently, we have a  
1689 direct partnership with each of the 18 critical  
1690 infrastructure and key resource sectors. Physically located  
1691 on the watch floor today we have representatives from the  
1692 energy sector, the financial services sector, the  
1693 communications sector, IT sector, Multi-State ISAC. We are  
1694 also finalizing agreements with chemical and others so they  
1695 can be physically present on the watch floor. In addition,  
1696 we recognize the unique capabilities of some of our other  
1697 partners in the manufacturing and antivirus environment. And  
1698 we are working with them to develop cooperative research and  
1699 development agreements so that they can be physically present  
1700 so that we can share data in real time.

1701           Mr. {Green.} Last week there were reports emerged about  
1702 a Department of Homeland Security report insider threat to  
1703 utilities, and when you mentioned utilities were involved in  
1704 it, do you have pretty well unanimous support or working  
1705 relationship with our utilities in our country from investor-  
1706 owned, municipal-owned co-ops like the TVA even? Is that  
1707 pretty well uniform throughout the country?

1708           Mr. {McGurk.} Yes, sir. We have very direct  
1709 connections with many of our private-sector partners. We  
1710 have spent a lot of time developing cooperative agreements

1711 with--for instance, there is an organization that is made up  
1712 of the 18 largest utilities in the United States and they  
1713 have a Chief Information Security Officer Panel, which we  
1714 interface with directly. I have personally briefed them on a  
1715 number of occasions and provided input into those  
1716 organizations so that they have a better cyber awareness.

1717       Mr. {Green.} Okay. I know the report was not released  
1718 to the public and in the news story we talked about, we have  
1719 a high confidence in our judgment that insiders and their  
1720 actions pose a significant threat to infrastructure and  
1721 information systems of U.S. facilities, and I understand,  
1722 like I said, the report is not made public. I would like to  
1723 ask some questions about insider threats to our utilities.

1724       Ms. Stempfley, could utility facilities be targets for  
1725 terrorists on the cyber side? We know physical targets.

1726       Ms. {Stempfley.} So I think you will find that the  
1727 vulnerabilities that exist and are possible to be exploited  
1728 exist in many places to include utilities across the board.  
1729 That is one of the reasons why, as we have reiterated, we try  
1730 to look at this from a common approach across the  
1731 environment.

1732       Mr. {Green.} I am aware in Texas and Houston we have  
1733 mostly investor-owned utilities, our service provider center  
1734 point, and I know they are doing some really great things,

1735 but does access to these sensitive facilities--mostly owned  
1736 by the private companies--need to be closer guarded and  
1737 carefully monitored to protect these threats?

1738 Ms. {Stempfley.} So best practice activities in the  
1739 cyber security systems are ones of multiple layers of  
1740 defense, which would include not just perimeter defense but  
1741 internal architecture approaches that separate sensitive data  
1742 from each other, rely on identity and other services. Those  
1743 kinds of best practices, which are widely available, should  
1744 be employed across the board.

1745 Mr. {Green.} I know a news story last week described an  
1746 insider sabotage in April in a water treatment plant in  
1747 Arizona where a disgruntled employee took control of the  
1748 control room to create a methane gas explosion. What is DHS  
1749 doing to ensure that these type of insider sabotage, again,  
1750 whether they are just one person or a plan, what is DHS doing  
1751 to try and limit some of these insider cyber sabotage?

1752 Ms. {Stempfley.} As we have identified, we continue to  
1753 provide the kinds of warning products, indicators of  
1754 activities that might be necessary and the kinds of best  
1755 practice guides for owners and operators to employ. In your  
1756 example, it would be up to that particular owner and operator  
1757 to employ those practices.

1758 Mr. {Green.} And Mr. Chairman, I would just like to ask

1759 one last thing.

1760 And do you get pretty good cooperation throughout the  
1761 country with the utilities?

1762 Mr. {McGurk.} Yes, sir, absolutely. We get a very  
1763 close working relationship with utilities.

1764 Mr. {Green.} Thank you, Mr. Chairman.

1765 Mr. {Stearns.} I thank the gentleman. We will quickly  
1766 go for a second round. We don't have votes and so I welcome  
1767 my colleagues if they wish to have a second round.

1768 I would like to return to the Stuxnet issue if you don't  
1769 mind, Mr. McGurk. If you can, just answer yes or no.

1770 Do you know how many operators in the industrial  
1771 controls infrastructure actually implemented DHS guidance on  
1772 Stuxnet?

1773 Mr. {McGurk.} No, sir.

1774 Mr. {Stearns.} Okay. How many U.S. companies use a  
1775 type of Siemens industrial-controlled products that were the  
1776 target of Stuxnet attacks?

1777 Mr. {McGurk.} A total number of companies? It is very  
1778 difficult to quantify, sir, because we don't have this  
1779 ability into all of their networks, but there were  
1780 approximately 300 companies that had some combination of  
1781 hardware and software.

1782 Mr. {Stearns.} So 300 U.S. companies?

1783 Mr. {McGurk.} Yes, sir.

1784 Mr. {Stearns.} Approximately. Good. Do you believe  
1785 that if the U.S. companies implemented the DHS guidance on  
1786 Stuxnet, they will be able to fend off a future attack from  
1787 this software?

1788 Mr. {McGurk.} Yes, sir, from this particular piece of  
1789 mal code.

1790 Mr. {Stearns.} In addition to this software, we have  
1791 heard that there are other vulnerabilities identified in  
1792 industrial-controlled systems, including a Beresford  
1793 vulnerability or exploit. Does that ring a bell?

1794 Mr. {McGurk.} Yes, sir.

1795 Mr. {Stearns.} Um-hum. Given that Stuxnet's impact and  
1796 the other vulnerabilities that exist, are you comfortable  
1797 that our country's industrial control systems are secure from  
1798 cyber attacks?

1799 Mr. {McGurk.} I think it is an evolving threat, sir, so  
1800 we have to continue to move forward and not focus on the  
1801 previous attacks.

1802 Mr. {Stearns.} Wasn't the Beresford attack developed by  
1803 one researcher in about 2-1/2 months? That is our  
1804 background. And what does that say about the safety of our  
1805 system if someone could work with his laptop computer in 2-  
1806 1/2 months, develop something that is vulnerable, and be

1807 used? Would you care to comment?

1808 Mr. {McGurk.} Yes, sir. What that really highlights is  
1809 the fact that it is not necessarily attributed to the actor  
1810 itself but it is the action and the vulnerabilities that we  
1811 need to focus on. Because as you had mentioned in your  
1812 opening statement and again when focusing on Stuxnet, it is  
1813 not the capability of the actor that necessarily brings about  
1814 the consequence. It is the actual vulnerability associated  
1815 that is being exploited, and that is really where the  
1816 Department is focusing much of its efforts.

1817 Mr. {Stearns.} Okay. What step has DHS taken to  
1818 prepare and defend against a Beresford type of attack to  
1819 industrial control system and has this guidance or other  
1820 direction been issued to the industry of the private sector?  
1821 And I will ask you later. Go ahead, Mr. McGurk.

1822 Mr. {McGurk.} Sir, the Department has produced a number  
1823 of specific actions and guidance associated with various  
1824 types of cyber risk and cyber threats but again, not focusing  
1825 on the actor or the activity but focusing on the  
1826 vulnerability and the necessary methods to secure the  
1827 networks. We actually will not only address that issue but  
1828 maybe the next-generation issue that could occur.

1829 Mr. {Stearns.} Do you actually talk to these U.S.  
1830 companies to see how they are implementing and doing this?

1831 Mr. {McGurk.} Yes, sir. In many cases, we are invited  
1832 to actually do an onsite assessment associated with the  
1833 vulnerabilities to see how they implement the mitigation  
1834 plans.

1835 Mr. {Stearns.} Well, just approximately how many do you  
1836 think you have assessed?

1837 Mr. {McGurk.} We have assessed approximately--this past  
1838 year we did 53. The year before we did about 40. These are  
1839 voluntary assessments. The year prior to that, another 30.  
1840 So we have done over 100 voluntary assessments and incident  
1841 response activities over the past 3 years.

1842 Mr. {Stearns.} Now, was that oriented towards the  
1843 Stuxnet or was it also involved with the Beresford?

1844 Mr. {McGurk.} It is involved with all types of  
1845 vulnerabilities, not just those two particular instances.

1846 Mr. {Stearns.} Mr. Wilshusen, do you mind commenting?

1847 Mr. {Wilshusen.} Well, in our reviews we often also  
1848 focus on the vulnerabilities of systems because that is what  
1849 the agencies or the operators can control. They can't always  
1850 control the threats that come their way, but they can control  
1851 how well they protect their systems and protect against known  
1852 vulnerabilities. And so that is one thing that we often look  
1853 at. And at the systems that we examine at a detailed level,  
1854 we typically find that they are vulnerable.

1855 Mr. {Stearns.} Ms. Stempfley, you had indicated in a  
1856 question 5 years ago are we more vulnerable today than we  
1857 were 5 years indicate, you seemed to indicate you didn't  
1858 think so. And I guess the question is based upon what I have  
1859 just given you some examples how a man in just 2-1/2 months  
1860 could come up with something that can make our system  
1861 vulnerable, I guess the question for each panelist, can you  
1862 explain how the cyber threats you are seeing now are  
1863 different from 2 or 3 or 5 years ago? And I will start with  
1864 you, Ms. Stempfley?

1865 Ms. {Stempfley.} So the cyber threats now are certainly  
1866 more sophisticated than they were several years ago. The  
1867 threats are focused more on individuals and very specific  
1868 activities. An example I have used is spear fishing is very  
1869 targeted to an individual. I received an email not too long  
1870 ago that appeared to be from my husband as a situation and it  
1871 was about a topic about college payment activities, and that  
1872 was identified and sent to me. And had I clicked on it, it  
1873 may have been something that was malicious. That is an  
1874 example of increased sophistication and increased focus that  
1875 exists.

1876 The number of vulnerabilities that have existed and the  
1877 kind of model that you presented where a researcher  
1878 identified a vulnerability and something that is already in

1879 existence, that vulnerability had been there from the  
1880 beginning. It was just recently identified. And so the  
1881 specific vulnerabilities have not increased in that scenario.  
1882 We are just more aware of it now and more able to respond.

1883 Our protective measures and protective guidance are  
1884 about building these infrastructures in a way that reduces  
1885 the exposure of those vulnerabilities and makes it less  
1886 likely for threat actors to be able to be successful.

1887 Mr. {Stearns.} And Mr. McGurk?

1888 Mr. {McGurk.} Yes, sir. I would also agree that, you  
1889 know, it is a matter of awareness and understanding the  
1890 interconnected nature of the--

1891 Mr. {Stearns.} But you don't see the cybersecurity  
1892 increasing in the last 5 years?

1893 Mr. {McGurk.} Do I see cybersecurity risk?

1894 Mr. {Stearns.} Threats increasing.

1895 Mr. {McGurk.} Threats, yes, sir, as a result of  
1896 exploiting those vulnerabilities because of the  
1897 sophistication and also the targeted nature. In the past we  
1898 were talking about just basic data ex-filtration from a very  
1899 broad audience. Now, we are seeing--in the RSA example that  
1900 was mentioned earlier--very specific, targeted attacks  
1901 against these aggregation centers.

1902 Mr. {Wilshusen.} And I agree, and I think you will

1903 continue to see more blended types of attacks that exploit a  
1904 number of different vulnerabilities in order to gain access  
1905 to its target.

1906 Mr. {Stearns.} So you would agree that the cyber  
1907 threats are more now than they were 5 years ago?

1908 Mr. {Wilshusen.} And more sophisticated.

1909 Mr. {Stearns.} Let me just close by this question. I  
1910 am not quite clear myself what this Beresford software does  
1911 or did. Can you describe, Mr. McGurk, what it does? Do you  
1912 know anything about it?

1913 Mr. {McGurk.} I don't have those specific details of  
1914 the analysis in front of me today, sir, so I couldn't really  
1915 comment on that.

1916 Mr. {Stearns.} Anybody?

1917 Mr. {Wilshusen.} No.

1918 Mr. {Stearns.} Okay. All right. My time has expired.  
1919 The gentlelady from Colorado.

1920 Ms. {DeGette.} Thank you very much, Mr. Chairman.

1921 First of all, I would like to ask unanimous consent to  
1922 put Mr. Waxman's opening statement in the record.

1923 Mr. {Stearns.} By unanimous consent, so ordered.

1924 [The prepared statement of Mr. Waxman follows:]

1925 \*\*\*\*\* COMMITTEE INSERT \*\*\*\*\*

|  
1926 Ms. {DeGette.} Thank you.

1927 So this is the perfect segue actually to just one  
1928 question I had of clarification. We are all throwing around  
1929 the words threat, vulnerability, and risk quite a bit today.  
1930 And Mr. Wilshusen, I am wondering as we prepare for our  
1931 subsequent hearings on these topics, you can just basically  
1932 describe for us whether there is a difference between those  
1933 three words and what the technical descriptions are.

1934 Mr. {Wilshusen.} Sure. Yes. And there is a  
1935 difference. A threat is basically any circumstance or event  
1936 that can potentially cause harm to an organization's  
1937 operations, assets, personnel, or whatever. A vulnerability  
1938 is a weakness in the security controls that are over a system  
1939 or network. There is actually a fourth component here before  
1940 we get to risk, and that is impact. What is the impact that  
1941 could occur should a threat, either a threat actor or an  
1942 event occur, exploit a vulnerability? What is the impact  
1943 that it could have? And then those three of those kind of  
1944 equate to what risk is.

1945 Ms. {DeGette.} Thank you. And are they all three  
1946 things we should be concerned about?

1947 Mr. {Wilshusen.} Yes, indeed. Absolutely. Threats are  
1948 what you try to guard against. The vulnerabilities are what

1949 you try to prevent and minimize by taking corrective actions  
1950 and implementing appropriate security controls. And you do  
1951 that in such a manner that you minimize the impact should  
1952 such a security incident occur. And so, yes, it is important  
1953 to think of all of them.

1954 Ms. {DeGette.} So you have heard both me and the  
1955 chairman and other members of this subcommittee talk about  
1956 this committee's jurisdiction. I am wondering if there is  
1957 any particular sectors of our jurisdiction that you think we  
1958 should look more closely at in subsequent hearings?

1959 Mr. {Wilshusen.} I think in terms of from a cyber  
1960 perspective, I think probably the key sectors would be  
1961 energy, electricity, both nuclear and other just because of  
1962 the interdependencies that they have with other sectors, IT,  
1963 finance and banking, and also communications would be I think  
1964 the four that are the most important just because of the  
1965 interdependencies that they have with the other critical  
1966 sectors.

1967 Ms. {DeGette.} Great. Thank you.

1968 Thank you very much, Mr. Chairman. I yield back.

1969 Mr. {Stearns.} I thank the gentlelady. I want to thank  
1970 the witnesses for their participation, their coming here this  
1971 morning.

1972 The committee rules provide that members have 10 days to

1973 submit additional questions for the record, the witnesses.

1974 And with that, the subcommittee is adjourned.

1975 [Whereupon, at 12:40 p.m., the subcommittee was

1976 adjourned.]