

STENOGRAPHIC MINUTES  
Unrevised and Unedited  
Not for Quotation or  
Duplication

JOINT HEARING ON AGENCY RESPONSE TO CYBERSPACE POLICY REVIEW

TUESDAY, JUNE 16, 2009

House of Representatives,

Subcommittee on Technology and Innovation

joint with the

Subcommittee on Research and Science Education

Committee on Science and Technology

Washington, D.C.

**Committee Hearings**

of the

**U.S. HOUSE OF REPRESENTATIVES**



**OFFICE OF THE CLERK**  
**Office of Official Reporters**

1 | YORK STENOGRAPHIC SERVICES, INC.

2 | HSY167.190

3 | JOINT HEARING ON AGENCY RESPONSE TO CYBERSPACE POLICY REVIEW

4 | TUESDAY, JUNE 16, 2009

5 | House of Representatives,

6 | Subcommittee on Technology and Innovation

7 | joint with the

8 | Subcommittee on Research and Science Education

9 | Committee on Science and Technology .

10 | Washington, D.C.

11 |       The Subcommittees met, pursuant to call, at 2:47 p.m.,  
12 | in Room 2318 of the Rayburn House Office Building, Hon. David  
13 | Wu [Chairman of the Subcommittee on Technology and  
14 | Innovation] presiding.

15 Chairman WU. This hearing will now come to order.  
16 Welcome everyone to this afternoon's hearing on the  
17 Administration's cyberspace policy review. This is the  
18 second of three hearings the Science and Technology Committee  
19 is holding on cyber security. Last week the Research and  
20 Science Education Subcommittee held a hearing on the research  
21 needs for improved cyber security, and next week my  
22 Technology and Innovation Subcommittee will hold a hearing on  
23 the cyber security activities of the National Institute of  
24 Standards and Technology and the Department of Homeland  
25 Security.

26 I have been long concerned by the lack of attention  
27 given to cyber security by the federal government and by the  
28 private sector. Previously, federal efforts were output  
29 oriented-focused on things like the number of programs, funds  
30 spent, or numbers of interagency working groups rather than  
31 outcome driven. I am pleased that the new Administration has  
32 made cyber security a top priority and is focusing efforts on  
33 achieving outcomes such as fewer breaches of federal systems,  
34 fewer cases of identity theft, and the security of smart grid  
35 systems and health IT systems.

36 In order to achieve these very, very important results,  
37 it is essential to first conduct a review of our federal  
38 cyber security structure and efforts. The Administration's  
39 cyberspace review does not make any brand new

40 | recommendations. However, it is valuable as a frank  
41 | assessment of current federal activities and a roadmap for  
42 | what needs to be fixed. In general, the recommendations  
43 | suggest improving interagency coordination and coordination  
44 | with the private sector, modernizing the research agenda, and  
45 | enhancing public education on cyber security.

46 |       By addressing each of these recommendations we are  
47 | laying the building blocks for our new, outcomes-based  
48 | approach to federal cyber security. The four agencies  
49 | appearing before the Committee today have a significant role  
50 | to play in creating that foundation. During today's hearing,  
51 | I hope to learn how each agency intends to improve its  
52 | current cyber security efforts in response to the  
53 | Administration's review. This information will help guide  
54 | the Committee's ongoing efforts to protect our Nation's data,  
55 | computer systems and its citizens.

56 |       [The statement of Mr. Wu follows:]

57 | \*\*\*\*\* INSERT 1A \*\*\*\*\*

58 | [The Hearing Charter follows:]

59 | \*\*\*\*\* INSERT 1 \*\*\*\*\*

60 Chairman WU. I want to thank our witnesses for  
61 appearing before us today, and now I would like to recognize  
62 Representative Smith for his opening statement.

63 Mr. SMITH. Thank you, Chairman Wu, and thank you for  
64 holding this hearing today to review the Administration's  
65 efforts to strengthen cyber security as outlined specifically  
66 in the White House's recently released Cyberspace Policy  
67 Review. While federal efforts to increase network security  
68 date back several years, they were brought to the forefront  
69 in early 2008 when President Bush formally established the  
70 Comprehensive National Cyber Security Initiative to deal with  
71 widespread and successful cyber attacks on federal networks.  
72 President Obama has committed to fully continue this effort  
73 under his Administration and emphasized its importance in a  
74 recent speech.

75 It seems the continuity across the Bush and Obama  
76 Administrations, as well as the increased attention being  
77 given to this issue in Congress, provide indication of a  
78 small but important advantage of where we were just a couple  
79 of years ago. Awareness of this problem and the need for  
80 action is now nearly universal. There is broad agreement on  
81 the seriousness and magnitude of our cyber security  
82 vulnerabilities and the complexity of the technical and  
83 policy challenges that must be addressed to overcome them.

84 However, while there is a consensus on the problem, we

85 | are still at the earliest stages of identifying and  
86 | implementing solutions, and we are working through relatively  
87 | unchartered policy territory as we do so. Accordingly, I  
88 | hope both Congress and the Administration will work to  
89 | balance the pressure to act quickly and aggressively on cyber  
90 | security with the need for thorough and deliberate  
91 | consideration of all possible courses of action.

92 |       To this end, as we hold these hearings and consider  
93 | legislative options later this summer, I hope to focus on  
94 | three broad areas of cyber security policy: (1) R&D. Are we  
95 | investing enough in R&D given its importance as the primary  
96 | driver of increasing security over the long term? (2)  
97 | DHS-led efforts to secure the dot-gov domain. Are we  
98 | confident that the reported \$30 billion price tag of this  
99 | initiative is appropriately focused and is its centerpiece  
100 | program EINSTEIN going to provide effective and lasting  
101 | security? And (3) private sector critical infrastructure.  
102 | What is the best approach to improving the security of these  
103 | networks? Do new regulations or liability protections make  
104 | sense or could they be counterproductive to our security  
105 | goals?

106 |       I hope today's hearing will serve to begin the process  
107 | of answering these questions. I thank the witnesses for  
108 | being here, and I certainly look forward to a productive  
109 | discussion. I yield back.

110 [The statement of Mr. Smith follows:]

111 \*\*\*\*\* INSERT 2 \*\*\*\*\*

112 Chairman WU. Thank you very much, Mr. Smith. And now I  
113 would like to recognize Representative Lipinski, Chairman of  
114 the Research Subcommittee, for his opening statement.

115 Chairman LIPINSKI. Good afternoon. I would like to  
116 thank Chairman Wu for joining me in holding this hearing. I  
117 look forward to working with him and other members of this  
118 Committee on the critical issue of cyber security.

119 Last week my Research and Science Education Subcommittee  
120 held a hearing on the state of cyber security R&D, and  
121 several of our witnesses emphasized the need for better  
122 partnerships and information sharing between the Federal  
123 Government and the private sector. We also discussed the  
124 challenges facing incentivizing agencies, companies, and  
125 individuals, especially those that don't face an immediate or  
126 obvious threat to adopt established best practices and to  
127 disclose breaches in security, and the expert panel echoed  
128 recent reports regarding concerns over lack of prioritization  
129 in the federal R&D portfolio.

130 One additional issue we discussed in last week's hearing  
131 was the importance of education. The panel emphasized that  
132 our IT workforce needs to be taught the skills necessary to  
133 incorporate security into software and systems from the  
134 beginning. But IT professionals are not the only ones who  
135 need to be better educated. The panel agreed that increasing  
136 the public's awareness of the risks and consequences of poor

137 security practices is also essential. People are the  
138 beneficiaries of IT but also the weakest link in IT security,  
139 and computer scientists need to team with social scientists  
140 to gain a better understanding of how humans interact with  
141 and utilize technology.

142 We need a cultural change in the ways that Americans  
143 practice their computer hygiene.

144 Now, today I look forward to hearing from our witnesses  
145 about their agency's responses to cyberspace policy review.  
146 As I said, this is a critical issue, and I am very happy that  
147 the Administration has focused in on it and we are doing so  
148 here on the Committee.

149 A secure and resilient cyberspace is vital not only for  
150 the Federal Government but for businesses large and small and  
151 for every single American. This goal can only be realized  
152 through our combined efforts and a multi-disciplinary  
153 approach to the problem. So all of our witnesses and their  
154 agencies will play a key role in maintaining this vital  
155 cyberspace. I want to thank the witnesses for taking the  
156 time to appear before us this afternoon, and I look forward  
157 to your testimony.

158 [The statement of Mr. Lipinski follows:]

159 \*\*\*\*\* INSERT 3 \*\*\*\*\*

160 Chairman WU. Thank you, Chairman Lipinski. And now I  
161 would like to recognize Mr. Ehlers for his opening statement,  
162 the Ranking Member of the Research Subcommittee.

163 Mr. EHLERS. Thank you, Mr. Chairman. As the last and  
164 probably least, I will try to keep my comments very short.

165 The security of our information is vitally important to  
166 all Federal Government entities and that includes the House  
167 of Representatives. Many of my colleagues are aware that our  
168 own networks are targeted daily by people and governments who  
169 would like to do harm to us or to our government or to find  
170 out personal information that has been provided to us by our  
171 constituents or other friends in other countries.

172 It takes strategic planning and organization to avoid  
173 and address these attacks. When considering the impacts of  
174 information security on policy development related to  
175 electronic health records, national defense and technology  
176 development, for example, it quickly becomes obvious how  
177 important trusted networks are to the public and to  
178 legislators.

179 All of the federal agencies testifying at the witness  
180 table today play a critical role in protecting the security  
181 of our systems while maintaining the necessary freedom to  
182 exchange unfettered communication.

183 I look forward to your comments on how the agencies are  
184 advancing the national cyber security efforts, and I expect

185 | to learn a great deal from each one of you today. Thank you  
186 | very much.

187 | [The statement of Mr. Ehlers follows:]

188 | \*\*\*\*\* INSERT 4 \*\*\*\*\*

189 Chairman WU. Thank you, Dr. Ehlers. If there are other  
190 members who wish to submit opening statements, your  
191 statements will be added to the record at this point.

192 And now it is my pleasure to introduce our witnesses.  
193 Ms. Cita Furlani is the Director of the Information  
194 Technology Laboratory at the National Institute of Standards  
195 and Technology. Dr. Jeannette Wing is the Assistant Director  
196 at the Directorate for Computer & Information Science &  
197 Engineering at the National Science Foundation. Dr. Robert  
198 Leheny is the Acting Director of the Defense Advance Research  
199 Projects Agency, and Dr. Peter Fonash is the Acting Deputy  
200 Assistant Secretary at the Office of Cyber Security  
201 Communications at the U.S. Department of Homeland Security.

202 The witnesses will have 5 minutes for spoken testimony,  
203 and your written testimony will be included in the record in  
204 their entirety. And when you complete you testimony, we will  
205 begin with questions. Each member will have 5 minutes to  
206 question the panel, and Ms. Furlani, please proceed.

207 | STATEMENTS OF CITA FURLANI, DIRECTOR, INFORMATION TECHNOLOGY  
208 | LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY  
209 | (NIST); JEANNETTE WING, ASSISTANT DIRECTOR, DIRECTORATE FOR  
210 | COMPUTER & INFORMATION SCIENCE & ENGINEERING, NATIONAL  
211 | SCIENCE FOUNDATION (NSF); ROBERT F. LEHENY, ACTING DIRECTOR,  
212 | DEFENSE ADVANCE RESEARCH PROJECTS AGENCY (DARPA); AND PETER  
213 | FONASH, ACTING DEPUTY ASSISTANT SECRETARY, OFFICE OF CYBER  
214 | SECURITY COMMUNICATIONS, U.S. DEPARTMENT OF HOMELAND SECURITY  
215 | (DHS)

216 | STATEMENT OF CITA FURLANI

217 |       Ms. FURLANI. Thank you, Chairman Wu and Chairman  
218 | Lipinski, Ranking Members Smith and Ehlert, and Members of  
219 | the Subcommittees. I appreciate the opportunity to appear  
220 | before you today to discuss our role in cyber security and  
221 | our perspective on the Administration's Cyberspace Policy  
222 | Review.

223 |       Through our work in information technology, NIST  
224 | accelerates the development and deployment of information and  
225 | communication systems that are reliable, usable,  
226 | interoperable, and secure. It advances measurement science  
227 | through innovations in mathematics, statistics, and computer  
228 | science and conducts research to develop the measurements and  
229 | standards infrastructure for emerging information  
230 | technologies and applications.

231 |       Many of our vital programs impact national security,  
232 | such as improving the accuracy and interoperability of  
233 | biometrics recognition systems and facilitating  
234 | communications among first responders.

235 |       Research activities range from innovations in identity  
236 | management and verification, to metrics for complex systems,  
237 | to development of practical and secure cryptography in a  
238 | quantum computing environment, to automation of discovery and  
239 | maintenance of system security configurations and status, and

240 | to techniques for specification and automation of access  
241 | authorization in line with many different kinds of access  
242 | policies.

243 |       As you are aware, beginning in the early 1970's, NIST  
244 | has developed standards to support federal agencies  
245 | information assurance requirements. Through the Federal  
246 | Information Security Act, or FISMA, Congress again reaffirms  
247 | NIST's leadership role in developing standards for cyber  
248 | security. FISMA provides for the development and  
249 | promulgation of federal information processing standards, or  
250 | FIPS, that are compulsory and binding for federal computer  
251 | systems. NIST's mission in cyber security is to work with  
252 | federal agencies, industries, and academia to research,  
253 | develop and deploy information security standards and  
254 | technology to protect information systems against threats to  
255 | the confidentiality, integrity, and availability of  
256 | information and services.

257 |       Consistent with this mission and with the  
258 | recommendations of the President's Cyberspace Policy Review,  
259 | NIST is actively engaged with private industry, academia,  
260 | non-national security federal departments and agencies, the  
261 | intelligence community, and other elements of the law  
262 | enforcement and national security communities in coordination  
263 | and prioritization of cyber security research, standards  
264 | development, standards conformance demonstration, and cyber

265 security education and outreach.

266 The national security community, a number of state  
267 governments, and major private sector organizations are also  
268 adopting the risk management framework and cyber security  
269 controls designed by NIST for the Federal Government. NIST  
270 is engaging industry to harmonize product assurance  
271 requirements to align with industry business models and  
272 system development practices.

273 We play a leading security role in supply chain risk  
274 management, health care information technology, the Smart  
275 Grid, biometrics and face authentication, next generation  
276 voting systems, and cloud computing. We work with the  
277 intelligence and counterterrorism communities to facilitate  
278 cross sector information sharing among federal, state and  
279 local government organizations. We team with the Department  
280 of Justice and the Small Business Administration in extending  
281 cyber security education and training beyond the Federal  
282 Government into the private sector.

283 For the first time, and as part of the ongoing  
284 initiative to develop a unified information security  
285 framework for the Federal Government and its contractors,  
286 NIST has included security controls in its catalog for both  
287 national security and non-national security systems. The  
288 updated security control catalog incorporates best practices  
289 in information security from the United States Department of

290 Defense, the intelligence community, and civil agencies to  
291 produce the most broad-based and comprehensive set of  
292 safeguards and countermeasures ever developed for information  
293 systems.

294 Under the provisions of the National Technology Transfer  
295 and Advancement Act, NIST is also tasked with the key role of  
296 encouraging and coordinating federal agency development and  
297 use of voluntary consensus standards and coordinating the  
298 public-private sector development standards and conformity  
299 assessment activities through consensus standards  
300 organizations. NIST will continue to conduct the research  
301 necessary to enable and provide cyber security  
302 specifications, standards, assurance processes, training, and  
303 technical expertise needed for securing the U.S. Government  
304 and critical infrastructure information systems to mitigate  
305 the growing threat. NIST will continue to closely coordinate  
306 with domestic and international private sector cyber security  
307 programs and national security organizations.

308 Thank you for the opportunity to testify today on NIST's  
309 work in the cyber security arena and our views on the  
310 President's Cyberspace Policy Review. I will be happy to  
311 answer any questions you may have.

312 [The statement of Ms. Furlani follows:]

313 \*\*\*\*\* INSERT 5 \*\*\*\*\*

314 | Chairman WU. Thank you, Ms. Furlani. Dr. Wing, please  
315 | proceed.

316 STATEMENT OF JEANNETTE WING

317 Ms. WING. Thank you very much. Good afternoon,  
318 Chairman Wu and Chairman Lipinski, Ranking Members Smith and  
319 Ehlers, and members of the Subcommittees. I am Jeannette  
320 Wing, and I am the Assistant Director of the Computer and  
321 Information Science and Engineering Directorate at the  
322 National Science Foundation.

323 I am delighted to have the opportunity to speak with you  
324 today about NSF's support for cyber security research at the  
325 frontiers of knowledge, investments that capitalize on the  
326 intellectual capacity of the best and the brightest in our  
327 Nation's colleges and universities, as well as their many  
328 partners in the private sector. The research outcomes  
329 generated with NSF support will undoubtedly contribute to the  
330 security, stability and integrity of our global cyber  
331 infrastructure for many years to come.

332 To begin, I would like to emphasize that many cyber  
333 security measures deployed today build upon the fundamental  
334 research outcomes generated decades ago. Thus, as the recent  
335 60-Day Cyberspace Policy Review concludes, a national  
336 strategy to secure cyberspace in both the near and the long  
337 term must include investments in fundamental, unclassified,  
338 long-term research.

339 Allow me to share with you just a few important

340 fundamental research contributions made to date by the open  
341 research community, many originally developed with  
342 applications other than security in mind.

343 Cryptographic schemes and cryptographic-based  
344 authentication, enabling today's internet commerce, such as  
345 on-line banking.

346 Program analyses and verification techniques, enabling  
347 early detection of software vulnerabilities, thereby often  
348 preventing cyber attacks such as phishing, worms and botnets.

349 Machine learning and data mining approaches are now used  
350 in filtering spam and detecting credit card fraud.

351 CAPTCHAs, the distorted text that only humans, not  
352 machines, can decipher, ensuring that it is indeed a human,  
353 not a bot, who is buying a ticket online.

354 These and many other research results developed with NSF  
355 funding are being used routinely in numerous corporations  
356 today. Moreover, NSF-funded projects have spawned start-up  
357 companies that bring critical technologies to the  
358 marketplace, creating new jobs, expanding the economy, and  
359 helping to secure cyberspace.

360 This year, NSF will invest almost \$137 million in  
361 cutting-edge research on the science and engineering of  
362 trustworthy systems. Our interdisciplinary Trustworthy  
363 Computing Program, is a significant component of this  
364 investment and supports more than 800 principal

365 | investigators, co-principal investigators, and graduate  
366 | students.

367 |       We contribute to the Comprehensive National Cyber  
368 | Security Initiative, CNCI, through this program with the  
369 | focus on three vital areas, the scientific foundations of  
370 | trustworthiness, privacy, and usability.

371 |       NSF coordinates its cyber security research and planning  
372 | activities with other agencies primarily through the  
373 | Networking and Information Technology Research and  
374 | Development program, NITRD, and the InfoSec Research Council.

375 |       We play a leadership role in both activities.

376 |       NSF and the academic community greatly appreciated the  
377 | opportunity to contribute to the 60-Day Cyberspace Policy  
378 | Review. We are pleased that the review recognizes the  
379 | importance of investments in both fundamental unclassified  
380 | cyber security research, the kind of research NSF supports,  
381 | and cyber security education. The review also recognizes the  
382 | importance of a strong academia-industry-government  
383 | partnership in which NSF plays a central enabling role.

384 |       For example, the NSF Science and Technology Center,  
385 | called TRUST, and three Cyber TRUST Centers, all work  
386 | directly with industry partners to speed the transition of  
387 | research outcomes into products and services.

388 |       Looking ahead, there are several areas ripe for  
389 | industry-university collaboration. First, industry has data

390 | that are otherwise unavailable to academics. Providing  
391 | access to real data, appropriately sanitized, anonymized, and  
392 | scrubbed, based on real adversaries and real users of  
393 | operational systems and networks will allow researchers to  
394 | test their theories and to gain new insights.

395 |         Second, industry has problems looming on the horizon  
396 | that they just don't have time to solve or they can't even  
397 | imagine because they are so focused on the present. These  
398 | are exactly the kinds of problems academic researchers can  
399 | work on, anticipating the threats of tomorrow so that when  
400 | they arrive, solutions will be ready.

401 |         In my testimony today, I have provided examples of the  
402 | ways in which NSF works with its partners in the Federal  
403 | Government, the private sector, and academe to catalyze  
404 | research advances in cyber security.

405 |         With robust sustained support for research in both the  
406 | executive and legislative branches, we have a unique  
407 | opportunity to increase our Nation's investments in  
408 | fundamental, open, long-term cyber security research.  
409 | Investing now for the future means a more secure future.

410 |         This concludes my remarks. Thank you very much.

411 |         [The statement of Ms. Wing follows:]

412 | \*\*\*\*\* INSERT 6 \*\*\*\*\*

413 Chairman WU. Thank you very much, Dr. Wing. Dr.  
414 Leheny, I am going to get you started, and Chairman Lipinski  
415 is going to take over for a while. Dr. Leheny, please  
416 proceed.

417 STATEMENT OF ROBERT LEHENY

418 Mr. LEHENY. Mr. Chairman, Subcommittee members and  
419 staff, thank you very much for this opportunity to discuss  
420 DARPA's programs, information assurance, and cyber security.

421 As I believe you are already aware, DARPA's mission is  
422 to invest in high-risk, high-reward technologies that create  
423 new capabilities for our military and information assurance,  
424 and cyber security are important elements in our current  
425 portfolio of programs. Let me begin today by commenting on  
426 the significance of robust secure self-forming networks to  
427 the defense department.

428 Like many commercial enterprises, the department is  
429 transforming to network centric operations, so DARPA's  
430 programs are focused on ensuring that these networks can  
431 operate independently in a robust and secure manner. We are  
432 interested in two types of networks, strategic high-speed  
433 optical and satellite based global networks, networks relying  
434 on commercial hardware technologies for the most part. For  
435 these types of networks, our focus is largely on operations,  
436 survivability under attack, and security.

437 At the other extreme are practical, largely wireless  
438 networks, networks directly supporting the war fighter on the  
439 front lines. Wireless networks present both hardware and  
440 software challenges. They must be agile and adaptive,

441 | capable of operating in any environment, as well as being  
442 | able to manage, defend, and heal themselves at speeds beyond  
443 | human capabilities. And they must be self-forming without  
444 | recourse to the infrastructure or cell towers of the  
445 | commercial provider.

446 |       As network capabilities become ever more essential to  
447 | operations, these networks above all else must be secure. We  
448 | will spend about \$127 million on information assurance and  
449 | cyber security in the current fiscal year, and we are  
450 | requesting an increase of more than 14 percent to \$164  
451 | million for 2010. While most of these investments are  
452 | targeted to software architecture and protocol issues, to  
453 | ensure networks are secure from the ground up, their  
454 | underlying hardware must also be secure. So in what is truly  
455 | a DARPA hard problem, we are investing in a program we call  
456 | TRUST, oddly enough the same name that the NSF for one of its  
457 | programs, but we are doing something completely different.  
458 | What we are doing is we are investigating methods for  
459 | detecting malicious features inserted into semiconductor  
460 | chips during their design and manufacture and programming.  
461 | All of these efforts focus on the department challenges, but  
462 | we believe our successes, as has been the case in the past,  
463 | will eventually impact commercial network technologies as  
464 | well.

465 |       At this time, perhaps our most visible program, one of

466 | particular interest to this Committee which we took on as  
467 | part of the Comprehensive National Cyber Initiative, is our  
468 | program to develop a National Cyber Range. Recognizing that  
469 | scientific progress has always been paced by advances in our  
470 | ability to observe, test and perform rigorous experiments, we  
471 | are designing this range to be a vehicle for a significantly  
472 | advancing progress in cyber understanding and capabilities,  
473 | to be a tool for rapid, realistic, and quantitative  
474 | simulation assessment of cyber technologies. Researchers  
475 | will be able to operate at either the classified or  
476 | unclassified levels and with many more nodes than current  
477 | cyber test ranges with highly automated tools and regiment  
478 | techniques, they will have access to revolutionary research  
479 | capabilities, capabilities that will allow rapid network  
480 | simulation under real-world conditions, enabling efficient  
481 | development and testing of information assurance and cyber  
482 | security strategies.

483 |         The program has three phases. In the current first  
484 | phase, we began by seeking ideas from multiple sources which  
485 | after a government panel review resulted in our placing seven  
486 | teams under contract to develop competing designs for  
487 | delivery later this summer. At that time, the government  
488 | team will evaluate and select the best among these designs to  
489 | continue into a Phase II program to produce a limited number  
490 | of prototype ranges. In a third phase, the most capable

491 prototype range will be further developed into the  
492 operational range to be completed in 2012. DARPA is managing  
493 the National Cyber Range development, but we will transition  
494 the completed range to another organization for operation.  
495 The details are a work in progress. Presently two government  
496 working groups are studying the issues. One is developing a  
497 technical vision and business model for the range operations.  
498 The other is focused on security issues for accrediting the  
499 range for use by all agencies across the government. In the  
500 end, I believe the range will operate like other national  
501 research assets with a panel to review and prioritize user  
502 proposals and an administrator to maintain facilities and  
503 facilitate research or access.

504       Regarding how we coordinate our research with other  
505 agencies, I can assure you that we actively coordinate our  
506 efforts. Two specific examples include the multi-agency  
507 participation in the development of the National Cyber Range,  
508 and our teaming with the NSF to organize two cyber security  
509 workshops this summer. But in general, in the process of  
510 developing new programs, our program managers routinely  
511 engage with their counterparts in other agencies to scope out  
512 the best way forward to achieve a specific research goal.  
513 Regarding the 60-Day Cyberspace Policy Review, this  
514 high-level document ranges over a wide variety of policy  
515 issues, but I note that it specifically recognizes the

516 | importance of innovation in achieving cyber security,  
517 | explicitly calling out the supply chain threat which our  
518 | TRUST program is addressing and the importance of modeling  
519 | and simulation capabilities that the NCR will enable.

520 |       In conclusion, as the department expands its net-centric  
521 | operation, information assurance remains a critical concern.  
522 | In dealing with this concern, we are committed to working  
523 | with organizations across the government to contribute to the  
524 | national goals for a secure cyberspace, and when the new  
525 | DARPA director is in place, refining our plans, programs and  
526 | budgets for cyber security will be high on our agenda.

527 |       I would be pleased to answer your questions.

528 |       [The statement of Mr. Leheny follows:]

529 | \*\*\*\*\* INSERT 7 \*\*\*\*\*

530 | Chairman LIPINSKI. [Presiding] Thank you, Dr. Leheny.

531 | I now recognize Dr. Fonash for 5 minutes.

532 STATEMENT OF PETER FONASH

533 Mr. FONASH. Good afternoon, Chairman Wu, Chairman  
534 Lipinski, and members of the Subcommittees. Thank you for  
535 the opportunity to discuss the White House's recently  
536 released Cyber Policy Review as it relates to the Department  
537 of Homeland Security's ongoing efforts to secure the federal,  
538 civil, executive branch networks and information systems and  
539 to coordinate activities focused on securing the Nation's  
540 critical infrastructure.

541 One of the greatest threats facing our Nation is a cyber  
542 attack to the critical infrastructure on which we depend.  
543 Our society relies on technology and telecommunications to  
544 support our economy and critical government functions. The  
545 cyber threats to these systems are real, growing, and  
546 evolving. They are large, diverse and range from independent  
547 unsophisticated opportunistic hackers to technically  
548 competent adversaries and nation states.

549 The Nation must be vigilant, proactive and innovative as  
550 it addresses and mitigates the service disruptions. The  
551 department's National Cyber Security Division, or NCSD,  
552 serves as the national focal point for cyber security on  
553 behalf of DHS. It works with the private sector and federal,  
554 state, local, tribal and international governments to assess  
555 and mitigate cyber risk and prepare for, prevent, and respond

556 to cyber incidents.

557       The Cyberspace Policy Review assesses the current state  
558 of U.S. cyber security policies and structures. Based on  
559 this assessment, future decisions will be made regarding U.S.  
560 cyber security policy and appropriate structures to execute  
561 it. It is anticipated that those decisions will focus on the  
562 following five key areas outlined in the Review which build  
563 upon existing programs and activities: (1) developing a new,  
564 comprehensive strategy to secure America's information and  
565 communications infrastructure; (2) ensuring an organized and  
566 unified response to future cyber security incidents; (3)  
567 strengthening public, private, and international  
568 partnerships; (4) investing in cutting-edge research and  
569 development; and (5) beginning a national campaign to promote  
570 cyber security awareness and digital literacy and to build a  
571 digital workforce for the 21st century.

572       Within those areas, a series of near- and mid-term  
573 actions are set forth. DHS and NCSA, working with  
574 interagency partners, are actively engaged in advancing these  
575 actions. As many of them align with current NCSA activities,  
576 such as cyber security-related information sharing with  
577 federal, state, local and private sector partners, supply  
578 chain risk management, cyber workforce development, and the  
579 promotion of cyber security through national public awareness  
580 and education efforts, NCSA's fiscal year 2010 budget request

581 provides further justification details on how DHS tends to  
582 grow and support these and other cyber security activities  
583 necessary to protect the Nation from cyber threats.

584 Before I address some of NCSA's current initiatives, let  
585 me emphasize that privacy and civil liberties considerations  
586 are at the center of our efforts. Protecting the privacy of  
587 Americans and their personal information is not just a  
588 priority, it is required by law and we take it very  
589 seriously.

590 DHS leads a multi-agency approach to coordinate the  
591 security of federal, civil, executive branch networks. The  
592 United States Computer Emergency Readiness Team, or US-CERT,  
593 serves as a central federal information security incidence  
594 center and is the focal point for the security of federal  
595 civil executive branch networks. Agencies report instances  
596 to US-CERT, and it guides agencies on enhancing detection  
597 capabilities and works with them to mitigate information  
598 security incidence. US-CERT compiles and analyzes incident  
599 information, shares the information with the operators of  
600 federal information systems. US-CERT provides products  
601 ranging from current and potential information security  
602 threats to alerts about vulnerabilities.

603 In addition, US-CERT is improving its capabilities to  
604 protect the federal enterprise in response to growing cyber  
605 threats, in large part to ramp up the current activities due

606 to the Comprehensive National Cybersecurity Initiative, or  
607 CNCI. Over the last year, DHS has led the CNCI effort to  
608 establish a front-line defense for federal executive branch.  
609 As part of this effort, DHS works with the Office of  
610 Management and Budget to reduce federal executive branch's  
611 external connections through the Trusted Internet Connection,  
612 or TIC, program. Consolidating such connections is the first  
613 step to creating front-line defense. As we reduce external  
614 connections, we will deploy EINSTEIN, an intrusion detection  
615 system, at trusted internet connections which will allow us  
616 to more effectively analyze malicious activity across federal  
617 executive branch networks. We also work with federal  
618 agencies to develop additional capabilities to detect and  
619 eventually prevent intrusions. Such collaboration will help  
620 inform the products necessary to provide actionable  
621 information to our critical infrastructure community.

622 In addition to coordinating the security of federal  
623 civil branch networks, we work with industry and government  
624 partners to secure the Nation's critical infrastructure  
625 networks. The vast majority of the Nation's cyber  
626 infrastructure is owned by the private sector. As such,  
627 cyber security is not exclusively a federal responsibility,  
628 and the key to our assured success is protecting cyber  
629 infrastructures' collaboration with the private sector. It  
630 is for this reason DHS will continue to strengthen and build

631 upon a public-private partnership framework created under the  
632 National Infrastructure Protection Plan, or NIPP. The NIPP  
633 was used for one of the CNCI initiatives whose focus is on  
634 improving protection of privately owned critical network  
635 infrastructure through public-private partnership. It is  
636 often referred to as Project 12.

637 State, local, tribal governments and international  
638 communities also play crucial roles in improving cyber  
639 security. Recognizing the contributions that can be made by  
640 leveraging such partnerships, DHS works with all levels of  
641 government and in the international community to help them  
642 increase awareness. DHS also works with other agencies to  
643 develop a plan for the retaining a skilled, trained  
644 workforce. We need to build the next generation of our cyber  
645 security workforce that will help us maintain a competitive  
646 advantage. Over the coming years, we will focus resources on  
647 the education and training of our current workforce and  
648 developing and recruiting new talent. DHS is also  
649 encouraging university programs and provides scholarships to  
650 promising students.

651 In conclusion, as a Nation becomes ever more dependent  
652 upon cyber networks, we must address cyber security  
653 strategically. Overcoming new cyber security challenges is a  
654 difficult task requiring a coordinated, focused approach to  
655 better secure the Nation's technology communications

656 | infrastructure. President Obama's Cyberspace Policy Review  
657 | reaffirms that cyber security is among the most significant  
658 | issues facing the Nation's economic and national security and  
659 | it solidifies the priority that the Administration places on  
660 | improving cyber security.

661 | Thank you for your time today. I appreciate the  
662 | opportunity to discuss the department's efforts in advancing  
663 | our cyber security posture. I would be happy to answer any  
664 | questions from the Subcommittee.

665 | [The statement of Mr. Fonash follows:]

666 | \*\*\*\*\* INSERTS 8, 9 \*\*\*\*\*

667 Chairman LIPINSKI. Thank you, Dr. Fonash. We will now  
668 move onto questions. Chairman Wu is down there. I am not  
669 sure if you want to take back the Chair here or lead off with  
670 questions or shall I go?

671 Chairman WU. Go ahead.

672 Chairman LIPINSKI. Okay. This Chair will recognize  
673 himself for 5 minutes to lead off with the questions. Dr.  
674 Wing, you know, I was there yesterday at NSF and meet with  
675 Dr. Bement and the AD's. Some of these things that I am  
676 going to ask about are not going to be a surprise to you or  
677 anyone actually who knows my background as a social  
678 scientist. I brought up in my opening statement that one of  
679 the most important things that I think is often overlooked  
680 and probably the weakest link that we have right now for  
681 cyber security is the general population.

682 Now, I want to lead off by asking, what is NSF doing  
683 right now in terms of research? What research is being  
684 funded by the NSF or where are you trying to, you know,  
685 search out for research that involves social science aspects  
686 of cyber security and facilitating collaboration between  
687 social scientists and computer scientists?

688 Ms. WING. Thank you for your question. It gives me an  
689 opportunity to speak about the Trustworthy Computing program  
690 which is one of the things I wanted to do when I got to the  
691 National Science Foundation, was to actually broaden the

692 | scope of what we were doing in cyber security to make sure to  
693 | include topics like privacy and usability, which absolutely  
694 | includes understanding social science and how humans behave,  
695 | how organizations behave.

696 |         And so one of the things we specifically did was to  
697 | broaden the scope of our Cyber TRUST Program to include  
698 | privacy and usability, to work with our social science  
699 | colleagues to make sure that, for instance, we have reviewers  
700 | from their communities looking at proposals that speak  
701 | directly to these kinds of issues. In fact, cyber security  
702 | is of course not just security, reliability, privacy, and  
703 | usability. It is not just the technical issues that all of  
704 | us scientists and engineers like to address, but there are  
705 | much broader issues like legal and ethical which, if you look  
706 | at the whole problem, we really need expertise from both the  
707 | scientific and engineering communities as well as these  
708 | less-technical communities.

709 |         So we are very much keen at the National Science  
710 | Foundation in looking at the broader picture.

711 |         Chairman LIPINSKI. Thank you, Dr. Wing. I want to  
712 | throw out a general question for each one of you actually  
713 | going along these lines to tell me what rules do you have at  
714 | your agency, what type of education do you do of your  
715 | employees so that they do not wind up practicing bad computer  
716 | hygiene at the agency? So we will start with Ms. Furlani.

717 Tell me if there is anything that you do along those lines  
718 for your employees.

719 Ms. FURLANI. Well, of course, because we write the  
720 standards for the Federal Government, we expect our employees  
721 to live up to a higher standard. So we do work very  
722 diligently with our Chief Information Officer to ensure that  
723 the understanding of what needs to be accomplished to protect  
724 the systems and the citizens that are interacting with us are  
725 deployed appropriately into the staff. So it is something  
726 that we pay a lot of attention to in probably a more unique  
727 situation than others.

728 Chairman LIPINSKI. Actually, I have a friend who works  
729 for NIST who was going around to places where you can get  
730 your pictures printed up. He was trying to get to see where  
731 he could find a certain--I don't know if it was a virus or  
732 what exactly it was, but he was trying to find places where  
733 he could pick that up because he knew that this was going  
734 around to just get a better handle on all of this. Thank  
735 you. Dr. Wing?

736 Ms. WING. Yes, at NSF we have a Secure Information  
737 Technology Awareness Program. Every single NSF employee is  
738 required to go through a training every year, and it covers  
739 all the topics from how to choose a good password to shutting  
740 down your machine to make sure that screens with confidential  
741 information are not displayed and so on. And there are

742 | policy documents about this thick that everyone is expected  
743 | to read. So we have a very serious--we take security very  
744 | seriously, and everyone goes through this training program.

745 | Chairman LIPINSKI. Dr. Leheny?

746 | Mr. LEHENY. DARPA is a relatively small agency with  
747 | under 200 government employees. We have a large number of  
748 | contractors that work within our environment. We have no  
749 | formal training program with regard to computer security, but  
750 | as an agency within the Defense Department, our computers are  
751 | a part of a larger enclave that is monitored very closely.  
752 | We have a very robust information resource directorate that  
753 | is available to help people work their way through problems  
754 | they might be having with their computers. And so far we  
755 | have been successful in locking large numbers--as you might  
756 | imagine, our computer system is regularly under attack, and  
757 | we have had good success at preventing those attacks from  
758 | having any adverse affect on the operations of our computers.

759 | Chairman LIPINSKI. Thank you, Dr. Leheny. Dr. Fonash?

760 | Mr. FONASH. Yes, sir. Thank you. First of all, we  
761 | follow all the FISMA best practices, and we closely follow  
762 | FISMA. Our CIO is the person responsible for making sure  
763 | those things are implemented across our department. We also  
764 | are very much into security awareness training, and we  
765 | annually require people to take security awareness. In fact,

766 I have to take that tonight when I get home.

767 We also have sort of eat our own dog food in the sense  
768 of what we do is again, I mentioned the TRUST internet  
769 connections, and we actually have two TRUST internet  
770 connections and we are moving to have all our network traffic  
771 go through those trusted internet connections. And we have a  
772 close relationship between our security operations center and  
773 our US-CERT. Thank you.

774 Chairman LIPINSKI. Thank you. My time is expired. I  
775 will now recognize Mr. Smith.

776 Mr. SMITH. Thank you, Mr. Chairman. For Dr. Fonash, if  
777 we could maybe discuss a little bit the prioritization of the  
778 defenses, and with the deployment of EINSTEIN I know that  
779 approximately five agencies right now have already been  
780 deployed with EINSTEIN, is that correct?

781 Mr. FONASH. We have deployed. The systems are not  
782 operational yet. We are actually right now in the process  
783 of--there are several agreements that have to be set up.  
784 There is the service-level agreement, there is a memorandum  
785 of understanding. So those have to go through legal reviews,  
786 and in particular we have to address privacy issues. So we  
787 actually physically have those things established at those  
788 locations, but we are working the legal issues at this point  
789 in time.

790 Mr. SMITH. And then following will be eventually all

791 agencies?

792 Mr. FONASH. Well, the idea is we are doing it in  
793 phases. What we are doing, first of all, is we are doing it  
794 at DHS, and that is one of the five agencies I included. And  
795 then where we are going to go is we are working now with  
796 Justice, Department of Agriculture, and State Department and  
797 NASA in terms of deploying trusted internet connections,  
798 actual, the physical EINSTEIN devices to those locations. We  
799 have also worked with GSA, and we actually put on contract,  
800 we actually made contract modifications working with GSA on  
801 the networks contract, and now agencies can go to the  
802 networks contract and get those services, trusted internet  
803 connection services, from the networks contract vehicle. And  
804 so we are actually working with the carriers right now, AT&T,  
805 Sprint, Verizon to get them so that they can provide the  
806 capabilities. For example, they have to have a secure  
807 facility to do this trusted internet connection. So right  
808 now the carriers are working those particular instances of  
809 what equipment they need to put in place so they can offer  
810 those services.

811 So that will be available to any agency that wants to do  
812 that. And then our next phase would deploy at 25 additional  
813 agencies and then the rest at some future point in time.

814 Mr. SMITH. And so can you speak to the prioritization  
815 and perhaps the need to deploy with every single agency?

816 Mr. FONASH. I think that clearly the larger the agency  
817 and the more--you know, beauty is in the eye of the beholder,  
818 sir. So let me say that. So each agency has to make its own  
819 determination how important it feels its need to get this  
820 trusted internet connection. We clearly at DHS have moved  
821 forward and actually have installed trusted internet  
822 connections. In addition to that, we believe that State and  
823 Justice and NASA and Department of Agriculture, key locations  
824 that needed those trusted internet connections, and then we  
825 have made available to anyone who feels that they have the  
826 need to immediately move to those contract vehicle. Those  
827 contract vehicles will be available and actually the services  
828 will be offered to use those capabilities through the  
829 networks contract, and that is the determination by those  
830 individual agencies as they want to move toward that  
831 capability.

832 And then we have a list of 25 other agencies that we can  
833 provide to you if you wish in terms of what we feel are the  
834 top 25--

835 Mr. SMITH. Okay. Thank you.

836 Mr. FONASH. --beyond that.

837 Mr. SMITH. Relating to privacy, I appreciate the fact  
838 that the President said, with emphasis, that he would seek  
839 not to include monitoring the private sector networks or  
840 internet traffic. Then in the New York Times last Saturday

841 | stated that senior Administration officials have admitted  
842 | those assurances may be challenging to guarantee and practice  
843 | and that some Administration officials have begun to discuss  
844 | whether laws or regulations must be changed to allow law  
845 | enforcement, military or intelligence agencies greater access  
846 | to networks or internet providers when significant evidence  
847 | of a national security threat was found. So I mean, maybe it  
848 | is easier said than done to say that no private sector  
849 | networks or internet traffic would be included in this.

850 |         How would you respond?

851 |         Mr. FONASH. What we do is because of the capabilities  
852 | that we have with EINSTEIN we are actually able to--we do not  
853 | track the individual personal part of the messages. What we  
854 | do is we drop that and what we do is we track information,  
855 | what is called header information, basically the information,  
856 | where it came from, where it is going to, and we also will  
857 | look at--if we also recognize code, we will have patterns. A  
858 | particular code, a particular program has certain pattern, a  
859 | bit pattern in it, so you are able to actually recognize for  
860 | example malware. So if you have Conficker traffic or some  
861 | type of malicious code going past, you can actually recognize  
862 | what is called the signature of that and pick that up. But  
863 | for example, we wouldn't get into the privacy of a person's  
864 | email unless there was some issue, a national security issue,  
865 | or something like that. But clearly what you can do is

866 | protect the privacy by looking at the header information, and  
867 | there will be issues about PKI capture as we go forward, but  
868 | we will address that. We will make sure we are doing that  
869 | linked up with the privacy people, you know, making sure we  
870 | are protecting the privacy of the individual.

871 |       Mr. SMITH. And do you suggest any legislative or  
872 | regulatory changes?

873 |       Mr. FONASH. I think that is something that needs to be  
874 | addressed as we go forward. At this point in time, I cannot  
875 | recommend it.

876 |       Mr. SMITH. You do not recommend it?

877 |       Mr. FONASH. I would not be one to say yes or no at this  
878 | point in time. I think that is an issue that needs further  
879 | study.

880 |       Mr. SMITH. Okay. Thank you.

881 |       Chairman WU. The gentleman from New Mexico, recognized  
882 | for 5 minutes.

883 |       Mr. LUJAN. Mr. Chairman, thank you very much. I know  
884 | that I read a lot in the testimonies about the need for  
885 | coordination. If you could briefly touch upon how you were  
886 | together, how the coordinating is working. If it is not  
887 | working, what suggestions you may have, and also if any of  
888 | you worked directly with any of the expertise that we have  
889 | within any of our NNSA laboratories.

890 |       Ms. WING. So let me take that question on coordination.

891 | The coordination happens at all levels, and the best  
892 | coordination happens in fact at the lowest level or with the  
893 | technical people, at different agencies working together,  
894 | informing each other about what each agency does in terms of  
895 | what we fund, what we actually do. So we have program  
896 | directors who talk to each other at the different agencies,  
897 | and we coordinate things like running joint workshops to  
898 | reach the academic community, the private sector jointly, and  
899 | that coordination works beautifully from my perspective.

900 |       We also have more formal techniques for coordination.  
901 | For instance, NITRD, Networking Information Technology  
902 | Research and Development Program, and specifically we have  
903 | been overseeing the senior steering group of the CNCI, the  
904 | National Cyber Leap Year that is happening right now, and we  
905 | are working very well together on that.

906 |       Let me also say as far as NSF goes, in working with  
907 | other agencies like DHS and DARPA, we are actually working  
908 | together on deploying a cyber security test beds. A couple  
909 | of the test beds that we jointly support with the other  
910 | agencies, like DHS and DARPA, are actually starting points  
911 | for DARPA's cyber range. So I think we coordinate quite well  
912 | together.

913 |       Mr. LUJEN. Dr. Wing, do you work at all with any of the  
914 | expertise at any of our NSA laboratories, that you are aware?

915 Ms. WING. They contribute to NITRD.

916 Mr. LUJAN. To which?

917 Ms. WING. NITRD.

918 Mr. LUJAN. And what is NITRD?

919 Ms. WING. The Networking Information Technology  
920 Research and Development program.

921 Mr. LUJAN. Okay.

922 Ms. WING. It is a coordination--an organization that  
923 coordinates over 13 federal agencies on networking  
924 information technology and research and development.

925 Mr. LUJAN. Okay.

926 Mr. LEHENY. I would support Dr. Wing's comments about  
927 how coordination occurs largely at the program manager  
928 working level. As you may be aware, DARPA is an agency that  
929 does almost all of its research activities outside the agency  
930 by contract. Over 90 percent of our budget goes out as  
931 contracts to industry, academia and federal laboratories.  
932 Specifically, Sandia, for example, is an active participant  
933 in many of our programs including the National Cyber Range  
934 Development that I spoke about in my oral testimony. I would  
935 like to point out that innovation and creativity in research  
936 is an individual property or characteristic of individuals,  
937 and it is not a type of activity that works well when it is  
938 driven from above. I like to characterize DARPA as a  
939 bottoms-up organization. It is not the case that I wake up

940 | in the morning and come into work and ask my secretary to  
941 | send me a program manager to manage great ideas I had  
942 | overnight. Rather, it is the case that I arrive at work,  
943 | open my email and find that one of my program managers is  
944 | trying to get on my calendar to come and tell me about his or  
945 | her great idea. And it is in that way that new ideas, new  
946 | programs, are created.

947 |       Of course, in order to support the argument for creating  
948 | a program, a program manager has to reach out to other  
949 | workers in their particular field in order to be able to put  
950 | together a case for why a particular program should be  
951 | started and executed, relying solely on their own internal  
952 | creation of the program idea. It is usually not a good way  
953 | to make a convincing case. You want to draw on as wide a  
954 | body of people familiar with the technology and the  
955 | challenges that the program is going to address that you  
956 | possibly can in order to make the strongest case that you  
957 | can.

958 |       Mr. LUJEN. Thank you, Mr. Chairman. As my time  
959 | expires, I want to see if I may be available, if time  
960 | permits, for a second round of questions. I would like to  
961 | still look a little bit more into the true collaboration with  
962 | the NSA laboratories. Not too long ago we did include an  
963 | amendment to NITRD to include our national laboratories  
964 | because there was a concern that maybe we weren't using the

965 | coordination as much as we should have been in the past. And  
966 | so I would like to explore a little bit more and specifically  
967 | pin down to the expertise that does exist within NSA with the  
968 | attacks that they experience on a regular basis and then a  
969 | few other questions I may have. So thank you very much, Mr.  
970 | Chairman.

971 | Chairman WU. Very good. We will come back to the  
972 | gentleman.

973 | Now, the gentleman from Michigan, Dr. Ehlers, recognized  
974 | for 5 minutes.

975 | Mr. EHLERS. Thank you, Mr. Chairman. And I have a  
976 | question for Dr. Wing, although any of you could try to  
977 | answer it if you wish. But I was surprised to discover  
978 | approximately six months ago that the number of students in  
979 | colleges and universities deciding to major in computer  
980 | science has gone down dramatically and also that there is not  
981 | that much interest in high schools in getting involved in.  
982 | Everyone likes to play with their computer, but not very many  
983 | are saying I would like to do this and build a better  
984 | computer some time in my life. Since you are at NSF, you  
985 | have access to all these data. What is happening? Is the  
986 | enrollment continuing to be down? I raise this in the  
987 | context of this hearing because if we are not producing the  
988 | right people, we are not going to get anywhere with our  
989 | discussions on cyber security, and particularly

990 implementation of new ideas and new approaches. Could you  
991 enlighten me on that?

992 Ms. WING. Yes, thank you very much for that question.  
993 It is a concern, of course, at the National Science  
994 Foundation and my directorate about the decline in  
995 enrollments in the computer science undergraduate level. We  
996 had seen a decline for the past few years, primarily because  
997 of the dot-com bust and other worries. But fortunately, this  
998 past year we actually saw an uptick, and the community at  
999 large is much more optimistic now about seeing the  
1000 enrollments go back up. So we are crossing our fingers and  
1001 hoping that that will be a trend, a positive trend.

1002 I do share your concern that we are not producing enough  
1003 trained and educated students in computing, not just because  
1004 they are likely the ones to be designing and building next  
1005 generation information technology systems that we are all  
1006 going to enjoy using on a daily basis, but we are working as  
1007 a community to try to increase the pipeline to increase--to  
1008 improve how it is we project what computer science is so that  
1009 we can attract the best and brightest to the field.

1010 Mr. EHLERS. I hope you are successful. It looks like  
1011 Dr. Leheny would like to make a comment, too.

1012 Mr. LEHENY. Yes. Thank you very much for this  
1013 opportunity. DARPA has no specific charter to advance  
1014 undergraduate or below education. However, we have two

1015 | programs that I would like to inform you about that I think  
1016 | are attempting to overcome some of the issues that you raise.

1017 |       The first program is one we call Computer Science Study  
1018 | Group. It is a program targeted to untenured, young faculty  
1019 | members in computer science, and it is a three-year program.  
1020 | Over the period of three years the support level for the  
1021 | individual in the program could reach as much as a million  
1022 | dollars, and as part of the program, we bring these  
1023 | individuals onto military installations and expose them to  
1024 | specific areas of interest to the Defense Department in the  
1025 | hope that we can encourage them to think about their research  
1026 | agenda in terms of solving the kinds of problems that the  
1027 | Defense Department has to deal with.

1028 |       Currently, with the three-year program, as I mentioned,  
1029 | we bringing in about 10 untenured faculty into the program  
1030 | each year. We currently have about 30 in the program. As  
1031 | you may be aware, a few years ago, we ran a series of what we  
1032 | called grand challenges which were targeted to demonstrate  
1033 | the ability of unmanned automobiles to navigate through  
1034 | difficult terrain. We found that there was an enormous  
1035 | amount of interest among students in that program and in  
1036 | participating in that program. And so we asked in our budget  
1037 | last year for a modest amount of funds, on the order of a  
1038 | couple million dollars, to create a special program that  
1039 | would reach out to high school students, particular students

1040 interested in things like robotics in an attempt to stimulate  
1041 interest among students and the kinds of problems that we  
1042 have to deal with. Thank you.

1043 Mr. EHLERS. Also the robotics FIRST program is--

1044 Mr. LEHENY. Yes, that is one of the groups that we  
1045 expect to be supporting.

1046 Mr. EHLERS. Dr. Wing, you have something else?

1047 Ms. WING. Yes, Mr. Ehlers. I forgot to mention one of  
1048 the programs that my directorate runs is called CPATH, and it  
1049 was recognized in fact by the 60-Day Cyberspace Policy Review  
1050 as a way to again address a problem that you are concerned  
1051 about, attracting the best and the brightest to computer  
1052 science. And the whole notion of the program is to really  
1053 revitalize the undergraduate curriculum in computer science.  
1054 And one of the things I am very keen on doing is to actually  
1055 do outreach to the K through 12 level because I do believe  
1056 that it is increasing the pipe even before they get to  
1057 college to explain what computing is all about and to get  
1058 them into the field. So I wanted to mention the CPATH  
1059 program. Thank you.

1060 Mr. EHLERS. Well, that is good. Thank you. And I try  
1061 to do my part. As members of Congress, we get invited to  
1062 speak in schools regularly, and whenever I speak in high  
1063 schools I always tell the students they have to choose their  
1064 subjects very carefully and they should not overlook math and

1065 science because when they get out and start looking for a  
1066 job, they will discover that they will either be a nerd or  
1067 work for a nerd and ask which they would prefer doing. And  
1068 of course, they don't believe that, and then I simply ask  
1069 them who is the richest man in the world? And finally the  
1070 light starts to dawn a bit.

1071 But you know, they just haven't heard this. They don't  
1072 realize it. They don't understand the possibilities. They  
1073 may love to play with their computer, even to do esoteric  
1074 things with it. But the thought of doing that as a career  
1075 doesn't always cross their mind, probably because they don't  
1076 have a contact with people who do that on a regular basis.

1077 Thank you very much. I yield back.

1078 Chairman WU. Thank you, Dr. Ehlers. The National  
1079 Science Foundation has data that indicates you are having  
1080 success in your efforts.

1081 The gentleman from New York, recognized for 5 minutes.

1082 Mr. TONKO. Thank you, Mr. Chair. Dr. Wing, the  
1083 investments that are made long-term wise in cyber security  
1084 research by our Federal Government and certainly by the  
1085 private sector can bear great benefits. How do you see us or  
1086 NSF facilitating and encouraging the transfer of research  
1087 from academia into that equation?

1088 Ms. WING. Well, this a very good question because it is  
1089 specifically relevant for cyber security, obviously.

1090 Academics can do their research, write their papers, produce  
1091 students, and so on, but what really matters in the end is  
1092 protecting and securing our cyberspace. And if the private  
1093 sector owns most of that, then there has to be this more  
1094 engagement between the academic community and the private  
1095 sector.

1096 NSF, as I mentioned, through the Science and Technology  
1097 Centers that we run here and the Cyber TRUST Centers that NSF  
1098 supports, has direct connections to industry. There are  
1099 industrial partners who serve on the advisory boards on all  
1100 of these centers and also--so they are formal mechanisms that  
1101 we have. Even the large awards that we grant through the PIs  
1102 or our normal programs, often those PIs will have connections  
1103 to industry.

1104 It goes without saying that a lot of the researchers,  
1105 especially in cyber security, want to see that their research  
1106 ideas are relevant and can help. And so they have a personal  
1107 motivation to actually work with industry. Some of the  
1108 techniques just get out there immediately. So for instance,  
1109 one of the results recently has been in developing secure web  
1110 browsers. And so now one of the open source web browsing  
1111 companies has picked up those techniques immediately. A part  
1112 of it is because many of the researchers have personal  
1113 contacts in industry, and these kinds of things transfer  
1114 informally but quickly.

1115 Another mechanism that is not formal but very useful is  
1116 many of the students, graduate students, that are funded  
1117 through NSF often take summer internships at companies like  
1118 Google and Microsoft and Yahoo and so on, and one of the  
1119 reasons that they do that is in fact how they can get access  
1120 to real data. So there is great incentive to actually do  
1121 that. Plus it is a very good opportunity for students to see  
1122 what it is like to do research in an industrial setting.

1123 So there is a lot of free flow of information in that  
1124 way, and it is easy for academics to talk to industry and get  
1125 ideas out there.

1126 Mr. TONKO. On the flip side, how do you envision the  
1127 private sector having the greatest influence or impact on  
1128 creating the research agenda for NSF? Do they have a way to  
1129 influence that agenda?

1130 Ms. WING. Well, our agenda is officially--it is  
1131 actually very much like what Dr. Leneny was saying. We are a  
1132 very bottom-up organization as well, and it is the academic  
1133 community that speaks to us as far as where they see the  
1134 frontiers of research going, where the frontiers of science  
1135 going, what the challenging science questions are, and they  
1136 come to us with brilliant ideas and say, well, this is where  
1137 the field is going. And in those conversations, we are  
1138 always engaging industry. So whenever we run these planning  
1139 workshops, industry is as invited as the academic community.

1140 | So even from the very beginning, we try to engage the private  
1141 | sector in these kinds of strategic, agenda-setting programs,  
1142 | processes. We of course have the National Science Board  
1143 | where there is industry input through the Science Board.  
1144 | That helps the Foundation, helps us set priorities. And then  
1145 | as I mentioned before, some of the larger centers that we  
1146 | fund, like the TRUST Center, and we actually have four Cyber  
1147 | TRUST Centers, have industrial members on the advisory  
1148 | boards.

1149 |         So there are formal and informal mechanisms that  
1150 | industry can use to provide input into the academic research  
1151 | agenda.

1152 |         Mr. TONKO. And is there room for a lot more  
1153 | participation from the private sector or do you think that  
1154 | the awareness is out there and it has been pretty much  
1155 | heightened in the last couple of years, or do you think there  
1156 | is room for improvement in that?

1157 |         Ms. WING. I actually think there is a heightened  
1158 | interest, so I have gotten specific queries from IBM, AT&T  
1159 | labs, besides the usual IT companies like Microsoft, Google,  
1160 | and so on. We interact with them very closely on all sorts  
1161 | of reasons. But specifically, I have been hearing from some  
1162 | of these companies that they would like to participate more  
1163 | in telling the academics what the real problems are and what  
1164 | they should be working on, and the academics, you know, can

1165 | listen.

1166 |       The other mechanism I forgot to mention is of course in  
1167 | our review process, through the panel reviews, through the  
1168 | committee of visitors that we have. We always have industry  
1169 | representatives there to help with the reviews so that they  
1170 | can give some sanity check. Well, that is an interesting  
1171 | problem, but it is not relevant for industry. They can also  
1172 | help in the committee of visitors also provide input on the  
1173 | portfolio of investments that we make.

1174 |       So there are a lot of ways in which industry, either  
1175 | informally or formally, provides input to NSF.

1176 |       Mr. TONKO. Thank you. Thank you, Chair.

1177 |       Chairman WU. Thank the gentleman. Mr. Smith,  
1178 | recognized for 5 minutes.

1179 |       Mr. SMITH. I am inclined to ask about the use and  
1180 | application of sanity checks, but maybe there is not enough  
1181 | time here. I am just teasing.

1182 |       Dr. Fonash, if you wouldn't mind further discussion  
1183 | here, when it comes to public-private partnerships, I was  
1184 | pleased that the President did say that the Administration  
1185 | will not dictate security standards for private companies but  
1186 | will instead collaborate with industry to find technology  
1187 | solutions. Is that your take on his comments, briefly?

1188 |       Mr. FONASH. Yes, sir, I believe that is correct. What  
1189 | we need to do is, you know, our mission right now is

1190 | predominantly focused on protecting the Federal Government  
1191 | and protecting the dot-mil domain and then working with our  
1192 | private partners, and in particular, our critical  
1193 | infrastructures and making sure that they are aware of the  
1194 | situation so we do a lot of information sharing, so we are  
1195 | working on information sharing programs so they are aware of  
1196 | the threat and so that they take the appropriate measures to  
1197 | protect the network. And I think it is the issue of  
1198 | the--appropriate level of security for the infrastructure  
1199 | depends upon if you are dealing with a critical defense  
1200 | contractor who has critical national security information and  
1201 | is protecting that versus Walmart protecting the latest sales  
1202 | price on their network. So it is a relative issue. It is an  
1203 | issue that is somewhat based on the business case, you know,  
1204 | in terms of what is the risk, and you have to do risk  
1205 | mitigation.

1206 | Mr. SMITH. Right.

1207 | Mr. FONASH. And so you put the appropriate investment  
1208 | in based on risk.

1209 | Mr. SMITH. In your testimony you mentioned  
1210 | public-private partnership objectives as being key. Could  
1211 | you elaborate on that and you know, really maybe define how  
1212 | we go about that? I mean, I know that we want to take care  
1213 | of government and then the private sector, but I think we  
1214 | need to acknowledge that already there is a great degree of

1215 | overlap there and already public-private partnerships do  
1216 | exist, and there is transfer of information across the  
1217 | internet between government and the private sector. So how  
1218 | do we sort through that and especially with the broadened use  
1219 | of the key objective being public-private partnerships?

1220 |       Mr. FONASH. So the Federal Government clearly does not  
1221 | operate in a vacuum. We do our business. You know, the  
1222 | critical infrastructure that we even actually use on our own  
1223 | networks is actually owned by the ISPs or commercial carriers  
1224 | such as Verizon or AT&T. So we heavily rely on the public  
1225 | infrastructure to provide us services, to provide us  
1226 | communications, for us to do our business. And so what we do  
1227 | is we actually have under national infrastructure protection,  
1228 | have set up a process where we work with the critical  
1229 | infrastructures in terms of protecting those critical  
1230 | infrastructures. And we, the National Cyber Security  
1231 | Division, is actually the sector lead for the IT  
1232 | infrastructure, and then within cyber security and  
1233 | communications is the sector for cyber security and  
1234 | communications is the national communications system, and  
1235 | that is actually the sector lead for communications. So the  
1236 | two critical communications and IT sectors is within that  
1237 | authority, and we work closely with industry to develop risk  
1238 | mitigation. We are actually developing right now an IT risk  
1239 | mitigation process, and we will publish that in the near

1240 future so there is actually a process where they can actually  
1241 look at the IT sector and determine, you know, how they do  
1242 risk mitigation. That is actually a process that we actually  
1243 developed with industry.

1244       Going back to the R&D, we actually work with industry.  
1245 There is actually an industry panel that works with us  
1246 closely as part of the--each of the sectors have a--there is  
1247 a government sector committee and there is actually a public  
1248 industry sector community. And within that industry sector  
1249 committee, there is actually a group that works with us on  
1250 the R&D portion. And they actually provide us what they  
1251 believe are the IT R&D requirements and the communications  
1252 R&D requirements which we then pass on to the R&D community  
1253 through our S&T directorate and also through attendance of  
1254 their appropriate meetings.

1255       So we work that way. We also work from an operational  
1256 point of view. We work for the US-CERT which provides--from  
1257 the US-CERT is the information sharing, information security  
1258 center that we run for the Federal Government. But we make  
1259 that information available to our private partners in terms  
1260 of the warnings. And we also are building upon something the  
1261 Defense Department started was Defense Industrial Base, if  
1262 you are familiar with the Defense Industrial Base. What that  
1263 is is through the contracting process at DoD--

1264       Mr. SMITH. We can maybe get into that. I just have

1265 | limited time here, and I was just wondering, you talked a  
1266 | little bit about critical infrastructure protection. Can you  
1267 | perhaps indicate whether or not there is any intent to take  
1268 | the critical infrastructure off of the so-called internet  
1269 | grid as a means of protection?

1270 |       Mr. FONASH. At this point in time, there are no plans  
1271 | to make it off the grid because for the most part, there are  
1272 | two reasons. First of all, the cost in terms of trying to  
1273 | make the government and private sector a private network.  
1274 | The cost is very large. It wouldn't be robust in many ways  
1275 | because--for example, because you have a separate network,  
1276 | you wouldn't have the robustness of the public network, and  
1277 | so I don't think there would be any--and then also from a  
1278 | security point of view, since you are really all using the  
1279 | same network--when you talk about the internet, you are  
1280 | really talking about AT&T, Verizon and Sprint. And so  
1281 | everyone uses those networks. So it is a common carrier  
1282 | perspective here. So it is very difficult to take it off  
1283 | grid. So what we have to do is work together with industry  
1284 | in making sure it is secure, and you can have portions of it  
1285 | that are more secure. So for example looking at DNSSEC is  
1286 | something that we're looking at and going toward and going on  
1287 | the trusted internet connection so that certain enclaves are  
1288 | more secure than others.

1289 |       Mr. SMITH. Okay. Tank you.

1290 Chairman WU. Thank you. Mr. Lujæn, recognized for 5  
1291 minutes.

1292 Mr. LUJÆN. Thank you very much, Mr. Chairman. Ms.  
1293 Furlani, I will begin with you. I have a few questions about  
1294 the role that NIST plays with the payment card industry, if  
1295 you can help me understand that and the coordination with  
1296 that and what requirements maybe NIST has established for  
1297 PCI.

1298 Ms. FURLANI. What we have is the national vulnerability  
1299 database which captures all the--which works with industry  
1300 and with government to provide data on what the  
1301 vulnerabilities are. And the PCI, the payment card industry,  
1302 decided to use that database as their mechanism to determine  
1303 whether their companies meet certain criteria. We don't tell  
1304 them what to do, but we provide the resources that they can  
1305 measure against and understand whether their criteria are  
1306 being met before they issue a payment card.

1307 Mr. LUJÆN. So let me see if I understand that  
1308 correctly. NIST does not mandate or prescribe any standards  
1309 if you will that PCI has to follow? They utilize your  
1310 database as a tool, but there is no requirement that NIST  
1311 provides for them, is that correct?

1312 Ms. FURLANI. We are not a regulatory agency except for  
1313 the standards for the Federal Government to use in their  
1314 cyber security.

1315 Mr. LUJEN. Are you aware of any organization that has  
1316 standards that the credit card industry has to follow in  
1317 protecting consumer information against cyber security  
1318 crimes?

1319 Ms. FURLANI. I am not.

1320 Mr. LUJEN. And Ms. Furlani, I am not, either. I have  
1321 looked into this. I just thought maybe there is something  
1322 out there. The reason I bring it up, Mr. Chairman, if there  
1323 is no objection, I would like to submit an article from the  
1324 National Journal 2709, The Cybercrime Wave, into the record,  
1325 that maybe we could review which outlines some of the  
1326 alarming rates of crime, security breaches that are  
1327 increasing year to year, money lost, Mr. Chairman, and I  
1328 would make this available to the Committee and make sure we  
1329 get a copy for the record if there is no objection, Mr.  
1330 Chairman.

1331 Chairman WU. No objection, so ordered.

1332 [The information follows:]

1333 \*\*\*\*\* INSERT 10 \*\*\*\*\*

1334 Mr. LUJEN. The reason I say that, Mr. Chairman, is as  
1335 we look at this, I couldn't agree more with some of our  
1336 colleagues. The coordination that must take place from a  
1337 public and private perspective to be able to protect  
1338 consumers' information when they are getting hit at enormous  
1339 rates, I think the average that an individual gets hit back  
1340 to 2007 anyway that was measured according to the article is,  
1341 depending on the type of crime, between \$3,000 and \$3,500,  
1342 but just depending on what it may hit. We all know that we  
1343 are trying to help people out more and more today, Mr.  
1344 Chairman, that are sometimes getting taken advantage of. And  
1345 this is an area where I think we could truly coordinate to  
1346 provide some of those needed protections. One of the things,  
1347 Mr. Chairman, that vendors, as an example, are required to do  
1348 is to actually keep the data and back it up. And those are  
1349 some of the areas where the largest breaches occur. The  
1350 article highlights a breach that most of us are familiar  
1351 with, at TJMaxx where I think it was 90 million records were  
1352 actually taken advantage of, and to see truly what the  
1353 requirement of the merchants are, vendors are, as we are  
1354 looking at this cyber security loophole or lapses sometimes  
1355 that take place to see what we can learn from there to be  
1356 able to help individuals out. This is something that we  
1357 touched on a little bit in our Homeland Security Committee  
1358 hearing not too long ago, Mr. Chairman. I thought it was

1359 | important to bring up.

1360 |         Lastly, Mr. Chairman, the reason that I asked the  
1361 | question about the coordination is the first item in the  
1362 | report says that we need to improve interagency coordination.

1363 |         And so I know that we read about this, and what I would ask,  
1364 | Mr. Chairman, if our witnesses today are able to provide us  
1365 | with any thoughts or ideas, whether they support that point  
1366 | that was brought up or if they have suggestions on what can  
1367 | be brought up. Ms. Furlani, before I go, I would just like  
1368 | to highlight the point I was trying to make earlier, Mr.  
1369 | Chairman, around the expertise that we have within some of  
1370 | our NSA laboratories who have to deal with cyber attacks on a  
1371 | daily basis. Not only do they have the sophistication from a  
1372 | technological perspective on some of the data sets that they  
1373 | have compiled with how we can combat some of these attacks,  
1374 | but they have an interface with the Government and private  
1375 | sector as well, especially because of the nature of them  
1376 | being classified and also being civilian organizations  
1377 | because of how they have been created and that we look to  
1378 | them to see how we could utilize that expertise. And with  
1379 | the time remaining, Mr. Chairman, I would go to Ms. Furlani.

1380 |         Ms. FURLANI. I would like to specifically mention the  
1381 | interagency coordination that has led to our new draft  
1382 | publication 853 which is the recommended security controls  
1383 | that can be cause for low-, medium-, or high-risk systems and

1384 | the agreement across, the Director of National Intelligence,  
1385 | CIO, the DoD, the Committee for National Security Systems,  
1386 | and of course, NIST so that there is one base line for all  
1387 | the Federal Government which enables the vendors to sell into  
1388 | the Government much more easily. And then the other agencies  
1389 | that have much higher security requirements than what NIST  
1390 | normally promulgates can set their standards higher than  
1391 | that. So this was just recently released, and it is a true  
1392 | outcome of the coordination, particularly in the response to  
1393 | the Cyber Security Review.

1394 | Chairman WU. Thank you very much, and I want to thank  
1395 | you all for appearing before the Committee this afternoon.  
1396 | The record will remain open for two weeks for additional  
1397 | statements from members and for answers to any follow-up  
1398 | questions the Committee may ask of witnesses. The witnesses  
1399 | are excused, and the hearing is now adjourned.

1400 | [Whereupon, at 4:05 p.m., the Subcommittee was  
1401 | adjourned.]

\*\*\*\*\*  
 SPEAKER LISTING  
 \*\*\*\*\*

EHLERS.	10	48	49	51			
FONASH.	30	39	40	41	42	43	44
	56	57	58	60			
FURLANI.	14	38	61	62	64		
LEHENY.	24	39	46	49	51		
LIPINSKI.	8	29	36	37	38	39	40
LUJAN.	44	45	46	47	61	62	63
SMITH.	5	40	41	42	44	56	57
	59	60					
TONKO.	52	54	55	56			
WING.	19	36	38	44	46	49	51
	52	54	55				
WU.	2	5	8	10	12	18	23
	36	44	48	52	56	61	62
	65						
YORK STENOGRAPHIC SERVICES, INC. 1							

\*\*\*\*\*  
 CONTENTS  
 \*\*\*\*\*

STATEMENTS OF CITA FURLANI, DIRECTOR, INFORMATION TECHNOLOGY  
 LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY  
 (NIST); JEANNETTE WING, ASSISTANT DIRECTOR, DIRECTORATE FOR  
 COMPUTER & INFORMATION SCIENCE & ENGINEERING, NATIONAL  
 SCIENCE FOUNDATION (NSF); ROBERT F. LEHENY, ACTING DIRECTOR,  
 DEFENSE ADVANCE RESEARCH PROJECTS AGENCY (DARPA); AND PETER  
 FONASH, ACTING DEPUTY ASSISTANT SECRETARY, OFFICE OF CYBER  
 SECURITY COMMUNICATIONS, U.S. DEPARTMENT OF HOMELAND SECURITY  
 (DHS)

PAGE 14

STATEMENT OF CITA FURLANI

PAGE 14

STATEMENT OF JEANNETTE WING

PAGE 19

STATEMENT OF ROBERT LEHENY

PAGE 24

STATEMENT OF PETER FONASH

PAGE 30

\*\*\*\*\*  
INDEX OF INSERTS  
\*\*\*\*\*

***** INSERT 1A *****	PAGE	3
***** INSERT 1 *****	PAGE	4
***** INSERT 2 *****	PAGE	7
***** INSERT 3 *****	PAGE	9
***** INSERT 4 *****	PAGE	11
***** INSERT 5 *****	PAGE	17
***** INSERT 6 *****	PAGE	22
***** INSERT 7 *****	PAGE	28
***** INSERTS 8, 9 *****	PAGE	35
***** INSERT 10 *****	PAGE	62