

1 Diversified Reporting Services, Inc.

2 RPTS GONZALEZ

3 HIF203160

4

5

6 PROTECTING COMMUNICATIONS NETWORKS AND IMPROVING CONNECTIVITY

7 WEDNESDAY, JULY 22, 2026

8 House of Representatives,

9 Subcommittee on Communications and Technology,

10 Committee on Energy and Commerce,

11 Washington, D.C.

12

13

14

15 The subcommittee met, pursuant to call, at 1:32 p.m. in
16 Room 2123, Rayburn House Office Building, Hon. Richard Hudson
17 [chairman of the subcommittee] presiding.

18 Present: Representatives Hudson, Allen, Latta,
19 Griffith, Bilirakis, Carter of Georgia, Pfluger, Obernolte,
20 Houchin, Goldman, Guthrie (ex officio); Matsui, Soto, Ruiz,
21 Peters, Kelly, Barragan, Carter of Louisiana, Menendez,
22 Landsman, McClellan, Castor, and Pallone (ex officio).

23 Also present: Representative Joyce.

24 Staff Present: Ansley Boylan, Director of Operations;
25 Michael Essington, Chief Counsel; Sydney Greene, Director of
26 Finance and Logistics; Noah Jackson, Clerk; John Lin, Senior
27 Counsel; Elaina Murphy, Professional Staff Member; Ryan

28 Murphy, Director of Member Services; Dylan Rogers,
29 Professional Staff Member; Timothy Trimble, Staff Assistant;
30 Hannah Anton, Minority Policy Analyst; Parul Desai, Minority
31 Chief Counsel; Waverly Gordon, Minority Deputy Staff Director
32 and General Counsel; Tiffany Guarascio, Minority Staff
33 Director; Brendan Lopez, Minority Press Assistant; Jaime
34 McCoy, Minority FCC Detailee; Dan Miller, Minority
35 Professional Staff Member; Andrew Souvall, Minority Director
36 of Communications, Outreach and Member Services; Johanna
37 Thomas, Minority Counsel; and Hannah Treger, Minority Staff
38 Assistant.
39

40 *Mr. Hudson. The subcommittee will come to order. The
41 chair recognizes himself for an opening statement.

42 Good afternoon, and welcome to today's hearing. We are
43 here to consider several bills that address important issues
44 facing our nation's communications ecosystem. These range
45 from securing our networks from foreign threats and robocalls
46 to improving how we connect our rural constituents.

47 We all know the frustration of receiving unwanted
48 robocalls. Americans received an estimated 4.3 billion
49 robocalls last month alone. Although some of these calls are
50 legal, calls that the recipient has consented to receiving
51 such as from a school or a pharmacy, illegal robocalls
52 continue to be a problem. In fact, fraud perpetrated against
53 Americans by illegal robocalls costs an average of \$22
54 billion annually, primarily affecting those who cannot afford
55 such losses.

56 Additionally, fraudulent robocalls make us distrustful
57 of legitimate callers, causing us to ignore calls from
58 unknown numbers and often miss important calls. Congress has
59 taken steps to address this problem. In 2019 we enacted the
60 Pallone-Thune TRACED Act. This law took important steps to
61 reduce illegal robocalls by requiring providers to implement
62 call authentication, increase fines for intentional
63 violations of the Telephone Consumer Protection Act,
64 authorize traceback efforts, and establish a Federal

65 interagency working group to combat illegal robocalls.

66 The FCC has also taken important steps to reduce illegal
67 robocalls, both in implementing the TRACED Act and by working
68 to block these calls from reaching our networks in the first
69 place.

70 Unfortunately, however, more still needs to be done.

71 Bad actors continue to develop new ways to enter our
72 networks. And many of these culprits are based abroad,
73 making them hard to track down. One of the bills we are
74 considering today will improve our efforts to identify and
75 catch these foreign bad actors and make it harder for their
76 calls to enter our networks. These are meaningful steps.

77 I want to make clear that I am well aware of the
78 difficulties that Congress and the Federal Government face
79 when trying to address this problem. Fraudsters do not allow
80 -- do not follow the law, and we must be mindful of imposing
81 new requirements that will only burden legitimate callers
82 while doing nothing to reduce illegal calls that harm us.

83 We are also considering legislation to improve our
84 efforts to connect our unserved and underserved rural
85 constituents. Closing the digital divide has long been a
86 priority for this Congress, but our efforts to accomplish
87 this goal has created a web of overlapping and duplicative
88 programs. In 2022 the Government Accountability Office found
89 that the Federal Government runs over 130 broadband programs

90 across 15 different agencies. This fragmented approach has
91 led to overbuilding and waste, not to mention confusion
92 caused by conflicting requirements and obligations.

93 GAO has recommended a government-wide strategy to better
94 coordinate and align these programs, and I am pleased we are
95 considering legislation to do that. One helpful development
96 in our efforts to deploy broadband is the FCC's Broadband
97 Map. Although not perfect, this map has significantly
98 improved our ability to identify who has broadband and who
99 does not. We can improve this map, and today we are
100 considering a bill that will help us identify agricultural
101 areas so we can ensure farmers have the connectivity they
102 need for things like precision agriculture and other modern
103 technologies.

104 I know full well the immense importance of connecting
105 unserved Americans. I am a proud member of the bipartisan,
106 bicameral Universal Service Fund Working Group, and I am
107 continuing to work with this group on reforms to ensure the
108 USF is sustainable for future generations. The USF is an
109 important tool in our efforts to ensure universal
110 connectivity, and I hope we can reach an agreement very soon.

111 As we continue to deploy and upgrade communications
112 infrastructure nationwide, we need the most advanced
113 technology to ensure they are efficient, resilient, and
114 secure. To accomplish this we can turn to our favorite

115 buzzword, "artificial intelligence'', AI. At a time when
116 threats to our network are at an all-time high, AI is a
117 crucial tool to fight fire with fire and ensure one of our
118 most critical systems is protected. Although AI is already
119 deployed throughout our networks in certain capacities, we
120 can always benefit from a greater understanding of how it can
121 be implemented to maximize security.

122 We have a lot of talk -- to talk about today, so thank
123 you to our witnesses for being here. I look forward to this
124 discussion.

125 [The prepared statement of Mr. Hudson follows:]

126

127 *****COMMITTEE INSERT*****

128

129 *Mr. Hudson. And I now recognize the ranking member,
130 the gentlelady from California, for her opening statement.

131 *Ms. Matsui. Thank you very much, Mr. Chairman. I am
132 glad we are holding this hearing to address two basic needs:
133 affordable broadband for every American and secure networks
134 people can trust.

135 Reliable communications connect students to classrooms,
136 patients to health care, and communities to lifesaving
137 emergency services. In the Sacramento region we see both the
138 promise of connectivity and the consequences when it falls
139 short. A family can live only 20 minutes from downtown
140 Sacramento and still lack the connection needed for work,
141 telehealth, and online learning. And for families in the
142 California delta, broadband is also essential for monitoring
143 irrigation, tracking changing weather, and getting crops to
144 market. That is why accurate data matters. We cannot
145 connect the right places when our maps fail to show where
146 service is actually needed. It is great that we are looking
147 at ways to improve our broadband maps and provide a clearer
148 picture of connectivity across agricultural areas.

149 But infrastructure alone will not close the digital
150 divide. A connection does little good when a family cannot
151 afford service or lacks the device or skills to use it. That
152 is why I co-lead the bipartisan, bicameral Universal Service
153 Fund Working Group with Chairman Hudson. We are working to

154 preserve and modernize the programs that connect rural
155 communities, schools, libraries, health care providers, and
156 low-income families. It is also why I introduced the Digital
157 Opportunity Foundation Act. This legislation will bring
158 public and private partners together to expand digital
159 skills, device access, and broadband adoption. We must
160 ensure the infrastructure we build actually improves lives,
161 and that every person has the skills and tools to make full
162 use of it.

163 We must also secure these networks. Communications
164 networks connect Sacramento's hospitals, utilities, schools,
165 and businesses. A cyber attack can interrupt medical care,
166 classroom instruction, electricity, and emergency response.
167 I have long worked to protect our communications networks
168 from untrusted equipment and support more secure technology
169 made here at home. I have also pushed to strengthen
170 cybersecurity protections for our schools and libraries.
171 That effort helped build momentum for the FCC's \$200 million
172 cybersecurity pilot program. But our schools and libraries
173 need sustained support to protect their networks and the
174 people who depend on them. That is why I will keep fighting
175 to secure long-term funding, including through the Universal
176 Service Fund.

177 The bills before us also take important steps such as
178 studying how AI can help identify malware and cyber threats

179 in real time, but AI can also create new security risks. We
180 need strong guardrails for both open source and proprietary
181 AI models, especially when they are used in our
182 communications networks and other critical systems. That
183 means rigorous testing, strong cybersecurity standards,
184 transparency, and clear accountability when systems fail or
185 are misused.

186 Finally, we need stronger protection from scams. Last
187 year Americans lost \$3.5 billion to imposter scams. This
188 includes scams that lure consumers through text and phone,
189 and AI now allows criminals to clone a loved one's voice,
190 impersonate a government official, or create a convincing
191 false emergency. The bills we are considering at this
192 hearing takes important steps toward protecting consumers
193 from illegal robocalls, but we have more work to do. That is
194 why I am working on legislation to prohibit fraudulent AI
195 impersonations and improve coordination among enforcement
196 agencies. Scammers should not escape accountability because
197 they are exploiting new technologies and targeting our most
198 vulnerable communities.

199 I look forward to working with my colleagues to
200 strengthen the bills before us today and keep every community
201 connected and secure.

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

203

204 *****COMMITTEE INSERT*****

205

206 *Ms. Matsui. And with that, Mr. Chairman, I yield back.

207 *Mr. Hudson. Thank you. And before I recognize the
208 chairman of the full committee, just for the record, during
209 the ranking member's remarks I received a robocall. And it
210 said, hi, my name is Reginald and I am giving you a call
211 about your installment loan application. I want to reach out
212 personally because you have been pre-approved for \$45,000,
213 blah, blah, blah. Just pretty timely.

214 [Laughter.]

215 *Mr. Hudson. The chair now recognizes the chairman of
216 the full committee, Mr. Guthrie, for five minutes for your
217 opening statement.

218 *The Chair. Thank you, thank you. You are pre-approved
219 for 45,000? That is good. So good afternoon, and I thank
220 Chairman Hudson. I appreciate you for holding this
221 legislative hearing on these very important topics.

222 Securing our communications system from bad actors has
223 been a longstanding and bipartisan priority for this
224 committee. Ranking Member Pallone, then Chairman Walden,
225 Representative Matsui, and I led this committee's effort to
226 rip and replace untrusted vendor equipment from our mobile
227 networks by passing the Secure and Trusted Communications
228 Network Act in 2019. Since then this committee has worked to
229 ban Chinese-manufactured drones by passing the Countering CCP
230 Drones Act. Just last year we passed Representative Latta's

231 ROUTERS Act to examine the threat of routers made in or by
232 countries of concern, including China.

233 That said, we remain vigilant to threats posed by
234 adversaries like China and are committed to protecting our
235 critical infrastructure and safeguarding Americans' data.
236 Recent reports of a China-linked plot to cripple New York's
237 communications networks serve as a stark reminder that these
238 threats are real and ongoing, and shows the lengths to which
239 our adversaries will go to undermine our interests and
240 threaten our homeland.

241 Given those risks, any legislation effort to amend the
242 Covered List administered by the FCC warrants careful
243 consideration by the committee. That is why today we will be
244 considering the GUARD Act, legislation that would add
245 humanoid and quadruped robots linked with certain CCP-linked
246 robotics companies to the Covered List. I appreciate the
247 work of the sponsors of the bill and the opportunity to
248 examine this threat today to better understand why Americans
249 should be concerned about humanoid and quadruped robots from
250 adversaries.

251 We will also spend time learning about other attack
252 vectors from adversaries such as malicious illegal robocalls
253 that are fraudulently attacking Americans. I don't know if
254 yours is fraud; you might be able to afford a \$45,000 loan, I
255 am not sure, but tacky. But it is interesting that happened

256 right as we are sitting here, isn't it?

257 And finally, legislation to ensure that Federal
258 broadband dollars are going to areas most in need.

259 Yes, I get the ones -- Kentucky doesn't have a DMV. We
260 call ours the transportation cabinet, so we just call it
261 transportation. So I keep getting the Kentucky DMV needs you
262 to call and give your money for tolls you haven't paid. And
263 one, we don't have hardly any toll roads. And second of all,
264 we don't have a DMV. But anyway, hopefully whoever is
265 sending me that doesn't figure out we don't have a DMV
266 because I know it is wrong and I don't owe any tolls.

267 So that -- so we are all affected, and we hear -- I hear
268 about this as much as anything from constituents back home.
269 I went to visit a friend of mine who I knew from early days
270 in politics who is now 87. And as we sat and talked for an
271 hour -- he has a home line -- I bet he answered at least six
272 or seven phone calls in an hour that were spam. So we need
273 to deal with this.

274 [The prepared statement of The Chair follows:]

275

276 *****COMMITTEE INSERT*****

277

278 *The Chair. And I will yield back.

279 *Mr. Hudson. Thank you. The chair now recognizes the
280 gentleman from New Jersey, the ranking member of the full
281 committee, for five minutes for his opening statement.

282 *Mr. Pallone. Thank you, Chairman Hudson, and today we
283 are examining legislation across a number of important areas
284 within the subcommittee's jurisdiction.

285 Network security continues to be a top priority for me
286 and this subcommittee, and we must stay on top of new and
287 emerging threats that use increasingly sophisticated
288 capabilities to compromise critical infrastructure. We have
289 watched closely as advancements in the tech space like AI-
290 powered coding and other recent innovations have
291 significantly reduced the time and labor costs for network
292 engineering and coding tasks.

293 Positive applications would be difficult to quantify,
294 but it is clear that widely available AI tools are empowering
295 individuals to build out applications, systems, and even
296 entire businesses virtually overnight without the need for
297 huge upfront capital investments. And fewer barriers to
298 entry for start-ups and small businesses could -- or should
299 open the door to more competition and choice for consumers.
300 But using history as a guide, we know that each innovation or
301 new capability that helps the good guys is also a tool that
302 can be used by bad actors for nefarious purposes.

303 Whether it is cyber criminals working alone or teams of
304 military or civilian personnel supported by adversarial
305 nations, our enemies can use the same capabilities to more
306 efficiently breach and sabotage American networks, and we
307 have to ensure that our network defenses stay ahead of the
308 curve.

309 With that in mind, I look forward to today's discussion
310 of the AI for Secure Networks Act, led by Representatives
311 Menendez and Pfluger, and to hear more about the ways we can
312 proactively employ AI to better defend our communications
313 networks from bad actors.

314 I am also interested to hear from witnesses about how
315 the GUARD Act led by Representatives McClellan and Moolenaar,
316 can apply the framework of my Secure and Trusted
317 Communications Networks Act to the rapidly-growing market for
318 humanoid and other robotics. Now is the time to act to
319 prevent untrusted suppliers with ties to our adversaries from
320 flooding the U.S. market with robotics and other advanced
321 technology and services.

322 There is also plenty of work to be done to address the
323 incessant robocalls and phone scams that still plague
324 consumers on a daily basis, despite all of our work on this
325 issue in the past. At best, robocalls and scams are a
326 nuisance. At worst, if executed successfully, they can upend
327 people's lives and cause thousands of dollars that are seldom

328 recovered from bad actors who seek out and prey on seniors
329 especially.

330 In spite of bipartisan efforts by Congress, the Federal
331 Communications Commission and the Federal Trade Commission
332 have both worked with carriers to weed out scam calls. But
333 my constituents continue to raise this issue as one in need
334 of our continued attention, and I hope today's discussion can
335 shed light on what obstacles are still preventing regulators
336 and law enforcement from stopping or reducing robocalls, and
337 I look forward to hearing from our witnesses about how
338 legislation like the QUIET Act and the Foreign Robocall
339 Elimination Act can help in these efforts.

340 We will also consider two pieces of legislation that aim
341 to build on the subcommittee's work to deploy broadband
342 infrastructure across the country so that every American can
343 access affordable and reliable high-speed internet service.
344 In particular, I hope to hear our witnesses' perspectives on
345 how the PLAN for Broadband Act led by Representatives Peters
346 and Walberg and the Data BRIDGE Act led by Representatives
347 Kelly Soho -- I mean Soto and Houchin -- can improve how we
348 manage, track, and carry out Federal broadband deployment
349 initiatives as efficiently as possible.

350 [The prepared statement of Mr. Pallone follows:]

351

352 *****COMMITTEE INSERT*****

353

354 *Mr. Pallone. So there is a lot to discuss, Mr.
355 Chairman. I yield back the balance of my time.

356 *Mr. Hudson. I thank the gentleman. I was distracted
357 because Reginald called again during your report, and
358 apparently I have been approved for another \$45,000 loan. So
359 this is this is amazing. This is incredible. I mean, this
360 is not that unusual, but I have gotten two robocalls since we
361 have started this hearing.

362 [Laughter.]

363 *Mr. Hudson. Mr. Allen wants to know what the interest
364 rate is.

365 Listen, we have now concluded with member opening
366 statements. The chair reminds members that, pursuant to the
367 committee rules, all members' opening statements will be made
368 part of the record.

369 We would like to thank our witnesses for being here
370 today and to testify before this subcommittee. Our witnesses
371 will have five minutes to provide an opening statement which
372 will be followed by a round of questions from our members.

373 The witnesses here before us today are Michael Robbins,
374 president and CEO of the Association for Uncrewed Vehicle
375 Systems International.

376 Thank you.

377 Kevin Rupy, partner with Wiley Rein, thank you for being
378 here.

379 Andrew Von Ah, director, physical infrastructure,
380 Government Accountability Office, thank you.

381 And Lindsay Gorman, former senior policy advisor for
382 technology strategy in the Biden White House.

383 Thank you for being here with us.

384 Mr. Robbins, you are recognized for five minutes for
385 your opening statement.

386

387 STATEMENT OF MICHAEL ROBBINS, PRESIDENT & CEO, ASSOCIATION
388 FOR UNCREWED VEHICLE SYSTEMS INTERNATIONAL (AUVSI); KEVIN
389 RUPY, PARTNER, WILEY REIN LLP; ANDREW VON AH, DIRECTOR,
390 PHYSICAL INFRASTRUCTURE, GOVERNMENT ACCOUNTABILITY OFFICE
391 (GAO); AND LINDSAY GORMAN, FORMER SENIOR POLICY ADVISOR FOR
392 TECHNOLOGY STRATEGY, BIDEN WHITE HOUSE

393

394 STATEMENT OF MICHAEL ROBBINS

395

396 *Mr. Robbins. Thank you, Chairman Hudson and Ranking
397 Member Matsui and distinguished members of the committee. It
398 is an honor to be with you today. I am Michael Robbins,
399 president and CEO of AUVSI. We are the trade association for
400 the autonomy, robotics, and drones industry. Our members are
401 at the leading edge of transformation, where artificial
402 intelligence, robotics, and autonomy are converging to create
403 a new frontier of cyber physical systems.

404 Before I turn to the GUARD Act, a brief personal word
405 because this hearing is very special for me. We are meeting
406 in the John D. Dingell room. I went to work for the late
407 John Dingell in 2002, when I was just 19 years old. And from
408 2006 to 2011 I had the privilege of serving as his chief of
409 staff. He was my boss, my mentor, and my friend. And much
410 of what I know about serving the public, including my
411 commission in the United States Navy, I learned from him.

412 With me today is my son. Like this room, he is named in
413 the congressman's honor, referencing Chairman Dingell's
414 family nickname of Jack.

415 Chairman Dingell used the jurisdiction of this committee
416 to defend American workers and consumers, and to keep our
417 industrial strength equal to our security. And that is the
418 argument I bring with you today.

419 AUVSI stands in strong support of the GUARD Act, and our
420 backing is informed by history and lessons from previous
421 policy failures in the drone industry.

422 Drone technology was invented in America. The scaling,
423 however, took place in China. Over a decade PRC
424 manufacturers came to dominate American skies. The PRC, the
425 People's Republic of China, leveraged massive state
426 subsidies, IP theft, and deliberate market dumping to drive
427 many American drone manufacturers out of business or keeping
428 their market share small by flooding the global market with
429 artificially cheap systems. That was market share engineered
430 in Beijing, not fairly earned in the market.

431 And this also injected considerable national security
432 risks into the United States. A Chinese drone is a flying
433 sensor built by companies that the PRC can compel to share
434 data that is collected back with the PRC. And that is why
435 CISA and the FBI have warned that Chinese drones put American
436 critical infrastructure at risk.

437 By the time Congress took action to address the risk and
438 the market imbalance, many American operators had built their
439 operations around a single foreign supplier. And therefore,
440 every policy option was costly and often faced with fierce
441 opposition from those who had become dependent on Chinese
442 technology. Nevertheless, we appreciate the courage of this
443 committee for moving forward.

444 The cost of restricting an adversary's technology is a
445 function of its installed base, and the installed base only
446 grows as the PRC executes on its deliberate strategy to
447 subsidize its companies and dump its products in the United
448 States to create strategic dependence. Accordingly, every
449 year of delay on robotics turns an easier decision into an
450 expensive and more complex one because the same PRC playbook
451 used for drones is now armed -- now aimed at robotics.

452 The humanoid and quadruped market is still relatively
453 new, only a few tens of thousands of units shipped worldwide
454 last year. But the capture dynamics are already visible.
455 Chinese firms already account for roughly 90 percent of the
456 global humanoid shipments. And our research universities,
457 where American robots once led, labs have shifted to
458 subsidized, artificially low-cost Chinese systems in just the
459 last 12 to 18 months. In public safety police departments
460 are adopting Chinese robot dogs in the same pattern that
461 entrenched Chinese drones over the last decade.

462 And like with drones, this is not merely an economic
463 contest; it is also a national security one. A compromised
464 laptop can expose data; a compromised robot can expose data
465 and also move, surveil, and act physically inside a factory
466 or a hospital or a power plant or on a military base. And
467 like with drones, under China's national intelligence law the
468 companies that build these systems can be compelled to serve
469 state intelligence in secret. Every such system is therefore
470 a Trojan horse on American soil.

471 The GUARD Act meets the moment because it is action
472 while the installed base for robotics is still small. It
473 protects our NATO and major non-NATO allies. It covers
474 finished systems and their software, not the components
475 American manufacturers source globally. And it pairs a
476 security review with a deadline that has consequences. AUVSI
477 supports the GUARD Act because it is important to note that
478 -- AUVSI supports the GUARD Act, but it is important to note
479 that it is just one half of a two-pronged strategy. It is
480 the defense.

481 Restrictions, by time, they do not win the entire
482 competition. The other half is offense. A national robotics
483 strategy like Congressman Obernolte has introduced secure
484 supply chains for critical inputs like rare earth magnets,
485 investment into U.S. research and manufacturing, and Federal
486 demand for trusted systems. We must protect and we must

487 promote.

488 Chairman Dingell spent his career getting ahead of
489 problems so the families he represented would not pay for
490 Washington's delay. When Chinese drones first arrived, no
491 one warned this committee where it would end because it had
492 not yet happened. This time with robotics we can see it
493 coming and we can act while it is still inexpensive to do so.
494 For my son's generation and for the American workers and
495 companies who will build these machines, I hope we will.
496 AUVSI oversee urges you to advance the GUARD Act.

497 Thank you, and I look forward to your questions.

498 [The prepared statement of Mr. Robbins follows:]

499

500 *****COMMITTEE INSERT*****

501

502 *Mr. Hudson. Thank you.

503 Mr. Rupy, you are recognized for five minutes for an
504 opening statement.

505

506 STATEMENT OF KEVIN RUPY

507

508 *Mr. Rupy. Chairman Hudson, Vice Chairman Allen,
509 Ranking Member Matsui, Chairman Guthrie, Ranking Member
510 Pallone, members of the subcommittee, thank you for giving me
511 the opportunity to appear before you today. My name is Kevin
512 Rupy, and I am a partner in the telecommunications, media,
513 and technology practice at Wiley Rein LLP. And I am here
514 today in my own personal capacity. All views expressed in
515 this testimony are my own.

516 I have worked to combat illegal robocalls and fraud
517 since 2012, including helping establish and oversee the
518 Industry Traceback Group, which has been the FCC's designated
519 traceback consortium since July 2020. I also serve on the
520 board of the Communications Fraud Control Association and
521 represent clients in efforts to combat illegal robocalls and
522 brand impersonation scams. I share the subcommittee's
523 concerns about illegal robocalls.

524 Consumer fraud, including illegal robocall schemes, is
525 no longer dominated by opportunistic scam artists.

526 Increasingly, it is carried out by sophisticated criminal

527 enterprises including transnational criminal organizations,
528 drug cartels, and hostile foreign actors operating at
529 industrial scale. As such, this issue raises serious
530 consumer protection and national security concerns, which is
531 why the subcommittee is right to focus on it. I would like
532 to make three points today.

533 First, enforcement works, especially when it is powered
534 by sophisticated tools including traceback. Federal, state,
535 and private civil enforcement actions demonstrated real
536 success in disrupting fraudulent schemes. Building on these
537 successes, the government should prioritize targeted and
538 meaningful enforcement actions. As scams become increasingly
539 tied to sophisticated criminal enterprises, Federal agencies
540 should fully deploy their criminal enforcement authorities to
541 combat this consumer protection and national security threat.
542 According to a recent Gallup survey, Americans lost an
543 estimated \$68 billion to scams in 2025 alone across multiple
544 channels, a level of consumer harm that demands an equally
545 aggressive criminal enforcement response.

546 Second, because fraud is highly dynamic, industry needs
547 flexible frameworks to adapt to evolving threats and respond
548 in real time. Fraud is most effective -- fraud prevention is
549 most effective when government and industry play to their
550 strengths. Government sets the general rules of the road
551 while industry responds quickly to emerging threats.

552 Accordingly, policy frameworks should preserve the
553 flexibility necessary for industry to innovate and respond as
554 threats evolve.

555 To this end, I urge Congress not to look to complicated
556 compliance frameworks like the TCPA as a solution to the
557 illegal robocall problem. The TCPA is an incredibly complex
558 statute already, and its core purpose is to establish
559 compliance guidelines for legitimate callers. Additional
560 compliance mandates will primarily burden legitimate callers,
561 not the scammers who routinely disregard the rules. I
562 encourage Congress to focus on legislation aimed directly at
563 fraudsters and criminal enterprises, rather than retrofitting
564 a compliance statute that bad actors will simply ignore.

565 Third, to keep pressure on illegal robocallers, industry
566 and government must strengthen collaboration and information
567 sharing. Fraudsters regularly collaborate across sectors;
568 defenders should, too. This collaboration is already
569 occurring on multiple fronts and is having meaningful
570 results. Information sharing and coordinated action across
571 telecom, financial, technology, and government sectors can
572 accelerate threat detection, disrupt fraud, and better
573 protect consumers from increasingly sophisticated fraud
574 schemes.

575 No single sector can combat fraud alone. Staying ahead
576 of evolving threats requires sustained information sharing

577 and coordinated action.

578 I look forward to discussing these issues with you
579 today.

580 [The prepared statement of Mr. Rupy follows:]

581

582 *****COMMITTEE INSERT*****

583

584 *Mr. Hudson. Thank you.

585 Mr. Von Ah, you are recognized for five minutes for your
586 opening statement.

587

588 STATEMENT OF ANDREW VON AH

589

590 *Mr. Von Ah. Chairman Hudson, Vice Chairman Allen,
591 Ranking Member Matsui, and members of the subcommittee, I am
592 pleased to be here today to discuss our work on Federal
593 broadband efforts as the committee considers potential
594 legislation.

595 Expanding and improving access to broadband across the
596 country has been a vexing and time-consuming task. Questions
597 about where to build, which technologies to support, and at
598 what cost to the taxpayer and price point for the consumer
599 have proven difficult to answer. Even then, other challenges
600 have presented themselves including difficulties in
601 interagency coordination, collecting accurate data for
602 mapping, and ensuring the viability of the networks we are
603 investing in, among other things.

604 In response to these many challenges, the PLAN for
605 Broadband Act being discussed today directs the development
606 of a national broadband strategy that focuses on improving
607 interagency coordination, reducing administrative barriers,
608 and ensuring funding is used efficiently and responsibly.

609 In May of 2022 we recommended the Executive Office of
610 the President develop and implement a national broadband
611 strategy to help agencies manage existing fragmentation and
612 overlap of the hundreds of broadband programs we identified,
613 focus Federal efforts on a common goal, and mitigate the risk
614 of potentially wasteful, duplicative efforts. At that time
615 Congress had created several new broadband programs and
616 increased funding for others in response to the pandemic,
617 which had underscored the importance of access to broadband.
618 Ultimately, four agencies -- FCC, NTIA, and the Departments
619 of Agriculture and Treasury -- administered the bulk of
620 broadband funding and have been executing programs to deploy
621 and support broadband.

622 Fast forward to today, and we are at a moment where
623 NTIA's BEAD program, the largest broadband deployment
624 program, is starting to roll out funding to states and
625 territories with the aim of connecting every remaining
626 location in the country. At the same time, the dozen or so
627 other broadband deployment programs administered by these
628 agencies are all in the middle of building out their projects
629 as well.

630 The question for our national strategy today may be more
631 about what comes next as we approach universal access over
632 the next several years. With or without a strategy, having
633 many overlapping programs creates the necessity for Federal

634 agencies to effectively collaborate to ensure they avoid
635 unnecessary duplication and meet the needs of unserved and
636 underserved communities. In April 2025 we reported that,
637 while the agencies have some processes in place,
638 opportunities exist to improve their efforts. For example,
639 clearly defining, agreeing upon, and documenting each
640 agency's responsibilities related to sharing the deployment
641 data and avoiding duplication would improve existing maps and
642 better position the agencies to sustain their collaborative
643 efforts, especially in the event of leadership or staff
644 changes.

645 Furthermore, we found that the agency's collaborative
646 efforts did not fully identify common outcomes or clearly
647 establish agency roles and responsibilities, including
648 leadership roles. To that end, the strategy called for in
649 the PLAN for Broadband Act calls for agencies to establish
650 those clear roles and responsibilities, as well as goals and
651 measures for their efforts.

652 Other work we have conducted has highlighted risks to
653 maintaining the broadband services deployed using Federal
654 funds, another factor that could be considered in the
655 creation of a national broadband strategy. For example, in
656 reporting on NTIA's tribal broadband program we found that
657 recipients were often relying on funding that was no longer
658 available in order to support subscribers. Without ensuring

659 whether recipients can afford to operate their networks, NTIA
660 risks the long-term viability of its investment. We have
661 ongoing work that we expect to issue later this year which
662 will discuss how agencies have addressed challenges
663 recipients face in maintaining broadband service.

664 Ensuring funding is targeted to areas of greatest need
665 also requires accurate data on where broadband is available
666 and where it is lacking. The Data BRIDGE Act being discussed
667 today also directs FCC to further refine its maps to identify
668 rural and geographically essential areas where broadband
669 deployment may be prioritized. Our work has highlighted the
670 importance of accurate maps and agency coordination efforts,
671 and in the targeting of Federal funding. Challenges to FCC's
672 data have frequently been successful, creating questions
673 about the overall accuracy of these maps. While FCC takes
674 steps to ensure the quality of its maps data, it has not
675 assessed how well those efforts are working. And in response
676 to our audit work and recommendations, FCC has taken some
677 steps to address issues related to data accuracy although our
678 recommendations remain open.

679 To sum up, as broadband deployment programs are in full
680 swing, our work suggests Federal agencies must continue to
681 effectively coordinate their efforts and improve the
682 broadband availability data they rely on to mitigate the
683 risks of overlap and duplication and risks that area of the

684 country remain underserved.

685 This concludes my statement. I look forward to any
686 questions.

687 [The prepared statement of Mr. Von Ah follows:]

688

689 *****COMMITTEE INSERT*****

690

691 *Mr. Hudson. Thank you.

692 Ms. Gorman, you are recognized for five minutes for your
693 opening statement.

694 Make sure your mike is on there.

695

696 STATEMENT OF LINDSAY GORMAN

697

698 *Ms. Gorman. Chairman Hudson, Ranking Member Matsui,
699 Chairman Guthrie, Ranking Member Pallone, and members of the
700 subcommittee, thank you for the opportunity to testify today.
701 My name is Lindsay Gorman, and I come from a background as an
702 AI and cybersecurity engineer with start-up companies, as a
703 builder with technology-focused venture firms, as a
704 researcher of U.S.-China technology and AI competition, and
705 as a former White House advisor on technology.

706 Two years ago I had the honor to testify before this
707 subcommittee on the future internet and the risks of cyber
708 warfare from the People's Republic of China. I argued then
709 that democratic allies needed trusted supply chains for a
710 projected \$500 billion Internet of Things market, and that
711 applications such as in health care and connected vehicles
712 introduce new risks around dependencies, building, espionage,
713 and intellectual property theft. Today those risks have
714 grown immeasurably, and they have also transformed in
715 character with the rapid adoption and diffusion of generative

716 artificial intelligence, yet the U.S. policy response has not
717 kept pace.

718 I focus my testimony on three dimensions of this
719 challenge: the new cyber attack surface posed by AI models,
720 agents, and applications; the competition with the PRC and
721 consideration of open versus closed AI; and advances in 6G
722 telecommunications networks as AI native.

723 First, AI is massively expanding the cyber attack
724 surface and risks, tipping the offense-defense balance in
725 favor of the attacker. AI systems are becoming increasingly
726 capable hackers. In April the UK's AI Security Institute
727 assessed that Claude's Mythos preview was capable of
728 autonomous intrusions. Just yesterday OpenAI announced that
729 during a benchmark cyber test its models escaped their test
730 environment, exploited a vulnerability to access the
731 internet, and breached fellow AI company Hugging Face to
732 steal the test results. Models and agents also create new
733 cyber access points for intruders such as through prompt
734 injection and data poisoning attacks. AI shows promise in
735 defending against cyber intrusions, but the barriers to
736 closing vulnerabilities are often less technical and more
737 organizational.

738 Moreover, as AI development moves from chatbots into the
739 real world, this attack surface will only grow. One movement
740 in AI community is the development of world models. In order

741 to realize the true superhuman intelligence its adherents
742 argue, AI needs to understand the physical, three-dimensional
743 world. The potential is extraordinary, from humanoid robots
744 that can diffuse explosive devices on the battlefield to
745 those that fold laundry at home. Just as with large language
746 models, enormous quantities of real world data will be
747 required to train these world models such as videos of
748 janitors cleaning office buildings, soldiers conducting
749 reconnaissance missions, factory workers assessing complex --
750 assembling complex machinery, or basketball players shooting
751 free throws. Once developed and deployed, these systems will
752 collect data continuously on their environments to refine
753 their models. A cybersecurity framework addressing covered
754 adversarial providers must contemplate this future.

755 Second, the United States and its allies can benefit
756 from leading open source AI infrastructure, but today it is
757 the PRC driving this approach. Historically, the United
758 States has enjoyed the benefits of open source leadership.
759 When software engineers the world over today write code, for
760 example, they do so in English. The U.S. holds a small lead
761 in frontier AI, but its infrastructural foundations are
762 unfolding behind closed doors. By contrast, PRC players are
763 releasing open weight models that are free to use but harder
764 to spot bugs. While analysts assess that this approach
765 carries -- is a short-term strategy while China lags behind

766 the U.S., it carries long-term risks that third countries
767 adopt PRC AI systems now due to cost. Some US companies
768 already are. The U.S. needs lower-cost alternatives for
769 export and a vibrant open source AI ecosystem at home.

770 Finally, 6G telecom networks will merge computing and
771 communications in an AI native architecture. The U.S. must
772 lead a coalition of democratic allies to deploy secure 6G as
773 foundational to secure global AI. In my written testimony I
774 provide recommendations to Congress to modernize U.S.
775 cybersecurity oversight for the AI era, secure AI models and
776 applications against foreign adversarial suppliers,
777 accelerate 6G adoption and security, secure and compete on
778 open source AI, and rebuild tech trust with allies and
779 partners.

780 The AI landscape is changing day by day and week by
781 week. Protecting our networks and our leadership is vital
782 for America's future.

783 Thank you, and I look forward to your questions.

784 [The prepared statement of Ms. Gorman follows:]

785

786 *****COMMITTEE INSERT*****

787

788 *Mr. Hudson. Thank you. We will now begin questioning,
789 and I will recognize myself for five minutes.

790 Mr. Rupy, I am tired of receiving illegal robocalls. I
791 got two while we were sitting here. My constituents are sick
792 of getting these calls. Many of these calls come from
793 abroad. So what can we do to find these perpetrators, and
794 how can we stop these calls from entering our network in the
795 first place?

796 *Mr. Rupy. Chairman Hudson, I share your frustration.
797 It is a huge issue. And, you know, I think based on, you
798 know, what I discussed in my testimony, I do believe we need
799 more enforcement and, in particular, criminal enforcement.
800 We need to find the bad actors behind this and put them in
801 jail. And the fact of the matter is we can do that. We have
802 powerful tools that, thanks to the TRACED Act, develop things
803 like the Industry Traceback Group, the Traceback Consortium,
804 STIR/SHAKEN call authentication.

805 So what I think we should be focusing on is directing
806 our efforts at identifying these bad actors and putting them
807 in jail, especially given the changing nature of this fraud.
808 It is no longer people operating boiler rooms. It is drug
809 cartels, transnational corporations. And the numbers are
810 just staggering. It is a national security issue, and
811 criminal enforcement warrants it.

812 *Mr. Hudson. I agree. So you mentioned in your

813 testimony about some of the consequences of -- if we get the
814 regulation wrong on this, and imposing too many burdens on
815 legitimate companies. Can you expand on that a little bit
816 more?

817 And why wouldn't -- you know, what is the harm that we
818 want to avoid by doing that?

819 *Mr. Rupy. Absolutely, Chairman Hudson.

820 I -- like, the way I think about this is where can we
821 get the most bang for the buck? And when I look at the TCPA,
822 in particular, has a role to play, right? It sets compliance
823 frameworks for legitimate callers who are trying to
824 communicate with consumers. But at the end of the day,
825 organizations like the Jalisco Drug Cartel and the Sinaloa
826 drug cartel, they are not going to play by those rules. And
827 the fact of the matter is the Jalisco drug cartel was
828 engaging in telemarketing.

829 So I think --

830 *Mr. Hudson. That is incredible.

831 *Mr. Rupy. -- you know, what we would be doing instead
832 of using a compliance statute to address this problem, this
833 is a criminal national security problem and we need to use
834 existing criminal statutes to address it.

835 *Mr. Hudson. Thank you for that.

836 Mr. Von Ah, it has been a few years since GAO released
837 its report on the need for broadband strategy to improve the

838 coordination of Federal broadband programs. Have things
839 improved over the last four years?

840 *Mr. Von Ah. Yes, I think things have improved. We
841 have seen programs get on track and begin putting money out
842 into -- to provide to carriers and others to build
843 infrastructure. So we have seen that. We have seen
844 improvements in agency coordination as well, better ability
845 to sort of de-duplicate or avoid duplication of effort where
846 they have overlapping service areas and things of that
847 nature. So yes, absolutely.

848 *Mr. Hudson. That is good news. With the BEAD program
849 finally connecting homes, do we still need 130 different
850 government programs doing broadband? Did we ever need that
851 many?

852 *Mr. Von Ah. Well, that is the question that we are
853 asking today with a strategy. I would say that we probably
854 don't need 130 programs, and BEAD's goal is ultimately to
855 connect every location that is in the map.

856 So what happens going forward, I think, is sort of the
857 next question for what we think of as a national broadband
858 strategy. What are the existing needs in a post-BEAD world?

859 *Mr. Hudson. Yes. Well, I agree with you on that.

860 Mr. Rupy, we have talked about how AI can be used to
861 secure our communications networks from bad actors. How are
862 providers using AI to combat illegal robocalls?

863 *Mr. Rupy. Thank you, Chairman Hudson.

864 Basically, think of it as an ecosystem. So we have
865 voice providers, we have partnering analytics providers. And
866 then, obviously, we have the bad actors. What I am seeing in
867 the industry right now is that these analytics providers are
868 using AI. They are using AI to make those algorithms that
869 they use to identify these calls more accurate. They are
870 using AI to identify AI-generated calls. And, you know, at
871 the end of the day this is a bit of an arms race. I mean,
872 the good guys are using AI and the bad guys are using AI.
873 But at the end, you know, basically, industry is leveraging
874 these tools because they are essential, particularly in this
875 space.

876 *Mr. Hudson. Well, I appreciate that, and that is just
877 one more reason we have got to win the race to develop AI.
878 You know, we have got to be the ones with the best systems.
879 Thank you for that testimony.

880 My time has expired. I now recognize the ranking
881 member, the gentlelady from California, for five minutes to
882 ask her questions.

883 *Ms. Matsui. Thank you, Mr. Chairman.

884 Cyber attacks are increasing in frequency and severity,
885 and AI models have increased the capacity for bad actors to
886 attack critical infrastructure. We need a clear strategy to
887 protect the communication systems that Americans rely on

888 every single day.

889 Ms. Gorman, many critical infrastructure providers rely
890 on complex networks with software from multiple vendors. How
891 could a trusted software catalog automated patching --
892 patching, and continuous monitoring help them close security
893 gaps?

894 *Ms. Gorman. Thanks for the question. As I had
895 mentioned in my testimony, AI is also creating this
896 incredible threat surface, but also can provide some
897 defensive tools, some of which you have mentioned in
898 automated threat detection, vulnerability patching.

899 What I would urge Congress to do is we really need to
900 have some minimum security standards when we are rolling out
901 networks. When we are using AI within our networks we need
902 to be sure that they are not subject to adversarial
903 incursion, and that can be -- they can be leveraged for these
904 benefits.

905 *Ms. Matsui. Okay. Can you suggest other tools that
906 Congress should support to help critical infrastructure
907 providers find and fix vulnerabilities faster?

908 *Ms. Gorman. I think, ultimately, some things -- some
909 of these things just have to be required. We can let the
910 private sector and collaborate with the private sector do
911 some of this on its own. But when it comes to critical
912 infrastructure, if AI systems are going to be discovering

913 vulnerabilities for the attacker, I think we need to require
914 that they are also going to be discovering vulnerabilities
915 for the defenders.

916 *Ms. Matsui. Okay. Open source AI supports innovation,
917 competition, and lower costs. However, they could carry, as
918 we know, significant risk if adopted without a clear
919 understanding of their origins or security limitations. Ms.
920 Gorman, how can Congress protect against unsafe AI models
921 while still allowing open source researchers and companies to
922 innovate?

923 *Ms. Gorman. There are two dimensions of the risk here.
924 One is models coming from adversarial actors such as the
925 People's Republic of China, which tend to be open weight.
926 And two is this question of can you audit the source code,
927 can you understand what a model is doing. Right now those
928 two questions are kind of aligned because the PRC is putting
929 forward these open weight models which, unlike open source
930 software traditionally, where you can inspect the source
931 code, you can see -- understand if there are bugs in there,
932 with open weight models that is not really the case.

933 So what the United States needs to do is, one, come up
934 with competitors to these low-cost models that the PRC is
935 putting forward; and two, support a vibrant open source --
936 not just open weight, but open source -- ecosystem for AI
937 infrastructure. Things like the national AI research

938 resource could be codified in statute, tools to develop the
939 infrastructure behind AI so that researchers across the
940 country can build on open source architectures for their own
941 models.

942 *Ms. Matsui. Okay. Now, Ms. Gorman, we know China is
943 making advanced AI models cheaper and easier to adopt. What
944 investments does the United States need to ensure that secure
945 American and allied alternatives remain affordable and
946 competitive?

947 *Ms. Gorman. Well, one way we could do this is right
948 now we have an American AI exports program where consortia of
949 AI providers and industry are coming together. And the idea
950 is they will receive preferential financing, maybe some tax
951 credits, investments, and also promotion from the State
952 Department around the world. We need to make sure that there
953 is a cost-competitive track of that, potentially open source,
954 potentially even open weight so that our systems can also be
955 in the global marketplaces competing directly with the PRC.

956 Not only do we need to make the best frontier models,
957 which the United States is still doing, but we also need to
958 be providing some lower-cost alternatives to meet the world,
959 I think, where it is.

960 *Ms. Matsui. Okay, all right. Well, thank you very
961 much, Ms. Gorman.

962 I yield back.

963 *Mr. Hudson. Thank you. The chair now recognizes the
964 chairman of the full committee, Mr. Guthrie --

965 *The Chair. Thank you.

966 *Mr. Hudson. -- for five minutes for your questions.

967 *The Chair. Thank you, Mr. Chairman. I am kind of
968 focused on the humanoid robotics industry.

969 So Mr. Robbins, who currently has the competitive edge
970 in the humanoid quadruped robotics industry, the U.S. or
971 China?

972 *Mr. Robbins. I would say the U.S. is leading the
973 innovation and China is leading in actual deployment.

974 *The Chair. Okay. Can you speak more about why you
975 think Congress needs to act swiftly?

976 *Mr. Robbins. Yes. The Congress needs to act swiftly
977 because we have seen the exact playbook that China is using
978 right now with humanoid and quadruped robotics and robotics
979 broadly worked very effectively in other industries like
980 drones, for example, which is an industry we also represent.
981 And the longer we wait, the more the installed base grows in
982 the United States. And the more difficult it is then to make
983 a policy change later, the more costly that policy decision
984 is to people who have installed the Chinese robots and built
985 that base. We saw that with drones when this committee
986 passed the protecting from CCP drone act, there was a lot of
987 opposition from people who had made significant investments

988 in Chinese drones, thinking that was okay. They didn't
989 understand the national security risk.

990 *The Chair. So what do you think are the concerns with
991 having these robots from China?

992 *Mr. Robbins. Yes, there is a couple of big concerns.
993 First, data exfiltration. The connected systems are, you
994 know, known to be directing data directly back to the PRC.
995 So when research is being done, that research in American
996 institution is also being shared with Chinese institutions.
997 So all of that leakage is occurring.

998 Further, there is -- these are mapping and surveilling
999 and audio sensors on all of these robots. So whatever
1000 operation they are in, whether it is a factory or a hospital
1001 or a military base, they are creating 3D models of the world
1002 around them. They are listening to the world around them.
1003 And again, all of that data can be leaked back to China. And
1004 then the scariest version is through a data update, a remote
1005 sensing -- remote access, they could actually be used to
1006 physically disrupt the environment that they are in, as well.

1007 *The Chair. Yes, this committee worked on the ban for
1008 Chinese cars, and that is the same issues with cars, as well.

1009 So also, Mr. Robbins, so prior to the GUARD Act's
1010 introduction, we worked with sponsors to add in a rule of
1011 construction to carve out partner and ally countries from
1012 being included in any addition to the Covered List. Can you

1013 talk more about the importance of collaborating with like-
1014 minded partners, specifically in the robotics industry?

1015 *Mr. Robbins. Absolutely, yes.

1016 *The Chair. And if we didn't have outside help -- I
1017 mean outside connections, not help, but connections.

1018 *Mr. Robbins. Yes, the robotics industry is a very
1019 global industry, and we have a very strong partnership in the
1020 United States with many democratic allied countries: Korea,
1021 Japan, Taiwan, throughout Europe, Israel, Australia. And we
1022 are much stronger when working together taking on China's
1023 authoritarian scale than when any single democratic nation
1024 trying to take on China's authoritarian scale alone.

1025 *The Chair. Okay. So also, Mr. Robbins, the Secure and
1026 Trusted Communications Networks Act I referenced earlier --
1027 we call rip and replace -- was signed into law in 2020.
1028 Since then, foreign-made -- this is the ROUTERS Act --
1029 foreign-made routers and drones have been added to the
1030 Covered List.

1031 *Mr. Robbins. Yes, sir.

1032 *The Chair. I guess that -- so since then, the foreign-
1033 made routers and drones have been added to the Covered. Are
1034 there any lessons learned that we should be considering as
1035 the GUARD Act goes through the legislative process?

1036 And for example, how should we think about balancing
1037 naming specific entities of concern versus entire categories

1038 of products and services?

1039 *Mr. Robbins. Yes, great question, sir. So when the
1040 FCC took action on drones, they did both. They named an
1041 entire category of products, drones. But they also named two
1042 particular companies, DJI and Autel Robotics, as particular
1043 entities, companies of concern, due to national security
1044 findings. So both work. In this case, in the robotics
1045 space, the leading Chinese robotics company, Unitree
1046 Robotics, has already had a national security finding from
1047 the Department of War. They have been placed on the 1260H
1048 List, which is the People's Republic of China PLA military-
1049 linked companies. So I think doing both would make sense in
1050 this case, as well.

1051 I think another lesson learned from drones that would --
1052 is a cautionary tale is with drones the focus was on all
1053 drones, not just on adversarial platforms. The GUARD Act is
1054 written in a way that targets verified national security risk
1055 with adversarial, and does not sweep in our trusted NATO and
1056 major non-NATO allies.

1057 Additionally, the GUARD Act also does not cover
1058 components; it instead has a study on components for
1059 potential future FCC action, allowing there to be more of a
1060 transition time for U.S. industry.

1061 *The Chair. Okay, I -- my time is about to expire. I
1062 got in all of my questions.

1063 I yield back. I appreciate it.

1064 *Mr. Robbins. Thank you, Mr. Chairman.

1065 *The Chair. Thank you.

1066 *Mr. Hudson. Thank you, Chairman. The chair now
1067 recognizes the ranking member of the full committee, Mr.
1068 Pallone, for five minutes for your questions.

1069 *Mr. Pallone. Thank you, Mr. Chairman.

1070 I believe my Secure and Trusted Communications Networks
1071 Act provided a helpful framework for how the FCC should work
1072 with our national security agencies to determine if certain
1073 communications equipment or services pose a threat to
1074 society. And under that framework the FCC must place the
1075 equipment or services that have been deemed a national
1076 security threat on its Covered List, which effectively
1077 removes them from our country's supply chains.

1078 But given these stakes, it is important for this
1079 committee to have oversight over the way the FCC is
1080 implementing the framework and ensure the FCC's decisions are
1081 the result of a rigorous and detailed national security
1082 analyst. So I have three questions of Ms. Gorman, and then I
1083 am going to go to one of Mr. Rupy.

1084 So Ms. Gorman, is it important for the FCC to work with
1085 our national security agencies to evaluate the security
1086 threats posed by communications equipment and services?

1087 *Ms. Gorman. Very. The FCC doesn't have a full picture

1088 on its own of national security threats.

1089 *Mr. Pallone. Okay. And should we build upon this
1090 framework to ensure that the FCC provides more transparency
1091 to this committee before placing equipment or services on the
1092 Covered List. And if so, why?

1093 *Ms. Gorman. I believe we should. We need a well-
1094 articulated strategy which the FCC should work with this
1095 committee, with Congress to develop so that the full spectrum
1096 of U.S. national security risks, as well as economic
1097 objectives, are considered in these decisions, and that the
1098 biggest risk can be mitigated with broad bipartisan support
1099 so that ultimately they stick.

1100 *Mr. Pallone. Okay. And then my third question is also
1101 how else can we improve the secure and trusted framework,
1102 especially given increasing capabilities of drones, of
1103 robots, and AI?

1104 *Ms. Gorman. I think we need to really clearly spell
1105 out what risks we actually want to guard against when it
1106 comes to securing our networks. We are about to be
1107 confronted with a huge panoply of PRC-made devices, robots,
1108 AI models, the systems using AI models, and we need to make
1109 decisions about what risks -- is it espionage? Is it
1110 dependance building? Is it intellectual property theft? Is
1111 it the pure cybersecurity risk that we want to guard against
1112 with these kinds of devices? And spell that out in a clear

1113 framework that looks to the future, that builds in both the
1114 network security and also the applications that are sitting
1115 on top of these networks.

1116 We are going to be using AI within the networks
1117 themselves. We are going to be training AI models on the
1118 network. So it is not enough to think about the applications
1119 and the networks as two separate pieces. But if we are going
1120 to be using AI to monitor network traffic for
1121 vulnerabilities, for malicious behavior, what are the
1122 guardrails we want to put on those systems? I think that is
1123 what this -- the -- an updated framework should get at.

1124 *Mr. Pallone. All right, thank you. I wanted to go to
1125 Mr. Rupy.

1126 We all know dangerous and unwanted calls and texts
1127 continue to bombard Americans. The TRACED Act, which I
1128 authored, required among other things the creation of the
1129 Industry Traceback Group, ITG, public-private partnership to
1130 trace and stop illegal calls. And while the ITG has helped
1131 to reduce the amount of unwanted robocalls, there is a lot
1132 more work in Congress -- for Congress and the industry to do
1133 here.

1134 So let me ask you first. Thank you for your past
1135 efforts to stand up the ITG. And with your experience, how
1136 else should the Federal Government and industry collaborate
1137 to further protect consumers from dangerous robocalls and

1138 robotexts, if you will?

1139 *Mr. Rupy. Thank you for that question, Ranking Member
1140 Pallone, and I applaud your leadership on the passage of the
1141 TRACED Act. When I think about the TRACED Act -- and I
1142 remember the run-up and the passage of it -- that is exactly
1143 the type of legislation that we need to be thinking about and
1144 how to approach this.

1145 You know, one of the big things that has changed since,
1146 you know, just prior to the TRACED Act and now is this
1147 involvement with criminal elements, national security
1148 threats. Like, it really has morphed in recent years, from
1149 my perspective.

1150 But I think, you know, to your point, the TRACED Act
1151 established the Traceback Consortium, the ITG, and the FCC --
1152 Federal -- other Federal and state agencies have used that
1153 data. ITG data fuels enforcement. And as an example, there
1154 was a case, the FCC-Sumco Panama, where once the FCC acted
1155 based on traceback data, those calls fell off a cliff. And I
1156 think what is missing is the individuals behind those calls.
1157 We need to bring criminal enforcement to this problem. I
1158 mean, the numbers are just staggering, particularly in terms
1159 of financial loss. So I think that is a key element.

1160 And collaboration is happening, and it works.

1161 *Mr. Pallone. All right. Thanks again.

1162 Thank you, Mr. Chairman.

1163 *Mr. Allen. [Presiding.] The ranking member yields, and
1164 now I will ask my questions here for the next five minutes.

1165 I want to thank Chairman Hudson for holding this
1166 important hearing, and I want to thank the witnesses for
1167 being here to testify.

1168 And we keep talking about robocalls. I have had my
1169 experience with those and, in fact, this one call I got, I
1170 mean, I told the guy, I said, you know, I am a Member of
1171 Congress and I am going to have the FBI investigate you. And
1172 he kept trying to get me to go buy this card at the -- and I
1173 finally said, did you hear what I said? And, you know, so I
1174 don't know, but, like I said, it sounds like a game of Whac-
1175 a-Mole, as far as these harassing calls, and they remain a
1176 nationwide problem. And they are getting really more serious
1177 and more serious, and I don't know where they come up with
1178 all these ideas.

1179 But obviously, we talked about some of the things that
1180 are working, but, you know -- and we talked about the TRACED
1181 legislation, where we can -- so we can trace these calls? We
1182 have the ability to trace these calls back to the originator?

1183 *Mr. Rupy. That is correct.

1184 *Mr. Allen. Okay.

1185 *Mr. Rupy. And one thing I want to emphasize about that
1186 is, prior to trace back, it would take months. Like, six,
1187 seven, eight months --

1188 *Mr. Allen. Okay.

1189 *Mr. Rupy. -- for law enforcement to do that. It can
1190 be done now in 24 hours.

1191 *Mr. Allen. Okay.

1192 *Mr. Rupy. Sometimes less.

1193 *Mr. Allen. So as far as convicting these people, where
1194 is the hold-up? Is it in the court system, or is it -- is
1195 law enforcement able to do what they need to do? Or is DoJ
1196 involved? How does that -- the court system work, and the
1197 fines, and things like that?

1198 *Mr. Rupy. So I think it is a resource issue.

1199 *Mr. Allen. Okay.

1200 *Mr. Rupy. I think it is a resource and prioritization
1201 issue.

1202 *Mr. Allen. Okay.

1203 *Mr. Rupy. And, you know, in my opinion, I think what
1204 often happens, whether it is a U.S. attorney's office, the
1205 DoJ, whomever, they see robocalls and they think, you know,
1206 this isn't a big deal.

1207 *Mr. Allen. Right.

1208 *Mr. Rupy. It is just robocalls.

1209 *Mr. Allen. Yes.

1210 *Mr. Rupy. But given the changing nature of this fraud
1211 and who is involved, I think there needs to be a
1212 prioritization on criminal enforcement. Civil enforcement

1213 works, it disrupts, it knocks them off their game, but I
1214 believe we need to put people behind bars.

1215 *Mr. Allen. How about the carriers and the equipment
1216 suppliers? What are they doing to try to eliminate this
1217 problem?

1218 *Mr. Rupy. So there are various things that are
1219 happening both, you know, on the handset side, on the carrier
1220 side. Carriers work very closely with various vendors that
1221 are providing more and more powerful tools to consumers to
1222 identify these calls.

1223 You know, traditionally these calls were being labeled
1224 with "scam likely'", "spam likely'". But as the fraud
1225 evolves, the tools evolve.

1226 *Mr. Allen. Right.

1227 *Mr. Rupy. And so now we are moving to solutions like
1228 branded calling solutions that, you know, will literally show
1229 verified number and logo --

1230 *Mr. Allen. Right.

1231 *Mr. Rupy. -- on the device. And carriers also work
1232 closely with the ITG in identifying these folks.

1233 *Mr. Allen. And so I am -- in listening to you, the
1234 Federal Government needs to do more to deal with this,
1235 obviously, in identifying these -- particularly, these --
1236 enforcing the laws outside your jurisdiction, because I am
1237 pretty sure this robocall I got was from some other country.

1238 I could barely understand the person.

1239 So, well, thank you for your work on behalf of that
1240 problem.

1241 Mr. Von Ah, in my district many communities don't care
1242 which Federal program builds broadband, they simply want
1243 reliable service. How can we make the Federal process easier
1244 for local providers, from electric cooperatives to local
1245 telephone companies in our communities that are just simply
1246 trying to get connected?

1247 GAO found that more than 130 broadband programs were
1248 spread across -- and I think the chairman mentioned this --
1249 15-something agencies. From your perspective, what is the
1250 single biggest coordination problem that Congress should be
1251 focused on fixing and getting this done?

1252 *Mr. Von Ah. So I think, from our work, Vice Chairman
1253 Allen, I would say that it is making sure that the roles and
1254 responsibilities amongst the agencies are clear. We have
1255 seen a lot of positive things from coordination. We have
1256 seen them focus on avoiding duplication and being largely
1257 successful in doing so. Less so are they sort of considering
1258 more strategic kinds of issues, whether that service is going
1259 to be sustainable over the long term, whether that is going
1260 to be -- you know, have the kind of subscribership that is
1261 going to sustain that going forward.

1262 And so we would like to see sort of, you know, what

1263 happens next with Federal agency coordination in those areas.

1264 *Mr. Allen. Yes, thank you. Well, I am out of time. I
1265 am over time, actually. Okay, I will now call on
1266 Representative Soto for his five minutes of questioning.

1267 *Mr. Soto. Thank you, Chairman.

1268 Technology is moving at an incredibly rapid pace, and
1269 this committee needs to keep up to help boost jobs, to lower
1270 costs, and protect our constituents. And so we have a
1271 wonderful hearing today on a whole range of issues from
1272 technology and telecommunications.

1273 First, continuing the battle against annoying and
1274 sometimes fraudulent robocalls, I feel like this is like the
1275 umpteenth chapter of that. But this time foreign calls and
1276 AI-generated voice calls are now on the menu finally, as
1277 well.

1278 Secondly, AI can be used to help, as well, in improving
1279 security and resiliency in our telecom network. I have seen
1280 that even in our local roads back home. So I am interested
1281 to see those efficiencies.

1282 And then stopping the flood of Chinese robotics. We
1283 know from our rip-and-replace issues with telecom from Huawei
1284 that Chinese companies have spied on us, they have used
1285 communist principles to help corner markets. We need to
1286 boost domestic production and make sure that we are -- these
1287 are trustworthy machines. Everybody wants a better cell

1288 phone service and internet connection, and so I know that
1289 when we are dealing with the AI telecom network bill that is
1290 going to be important.

1291 I am particularly excited about the Data BRIDGE Act,
1292 adding agriculture areas to national broadband maps. I am
1293 proud to represent cattle and citrus country. They are using
1294 precision agriculture, they are tracking livestock, receiving
1295 and analyzing large amounts of data to improve yields. And
1296 so that connectivity is so important.

1297 First, Mr. Von Ah, in relation to the Data BRIDGE Act, I
1298 have got to ask. Why were ag areas not included in the
1299 original National Broadband Map? Do you happen to know?

1300 *Mr. Von Ah. They were included in the sense that there
1301 -- if there is a broadband-serviceable location it would be
1302 included in the map. So for example, if there was a
1303 farmhouse, that would be a broadband-serviceable location.
1304 But it wouldn't necessarily show the entire area that might
1305 need broadband coverage.

1306 *Mr. Soto. Sure. And a lot of these farms and ranches,
1307 they are so vast that they are going to need different
1308 stations for both internet connections and for WiFi.

1309 On the BEAD program, we finally got testimony that two
1310 states, after a year-and-a-half into this Administration,
1311 finally are getting broadband. Do you see -- is the speed
1312 picking up finally again on some of the BEAD? Because I know

1313 Floridians, especially in these rural areas, are really,
1314 really waiting on this.

1315 *Mr. Von Ah. From all indications, it looks like
1316 funding is starting to go out. Nearly all of the state plans
1317 have been approved. And as you mentioned, there is funding
1318 going out the door to various states, and they are beginning
1319 to execute their plans.

1320 *Mr. Soto. Thank you so much.

1321 Mr. Robbins, I know under the GUARD Act we would help
1322 boost domestic production and also with our allies. So I
1323 guess my question is, would we be ready to meet the need or
1324 at least get close to meeting the need on day one?

1325 What would that look like, as far as having the means of
1326 production to be able to meet the demand for all these
1327 robotics that are needed for our daily lives?

1328 *Mr. Robbins. Yes, thank you for that question,
1329 Congressman.

1330 American robotics companies are actively working to
1331 scale manufacturing in the U.S. now, and working with
1332 partners from allied nations as well. The challenge at the
1333 moment is it is hard to scale when you don't have consistent
1334 demand, and it is hard to raise money when investors look at
1335 the marketplace and look at other markets where China has
1336 come in and dumped subsidized products into the market and
1337 drove American companies out of business.

1338 So right now investors are standing on the sidelines
1339 more than we would like them to. You know, private capital
1340 has sort of learned lessons from the drone industry, and
1341 solar panels, and others and said, you know, until the U.S.
1342 actually does something about this Chinese dumping, this
1343 might not be a safe bet. So addressing this now with the
1344 GUARD act would certainly help spur U.S. manufacturing, as we
1345 are seeing now in the drone industry, where there are
1346 literally hundreds of millions of square feet of drone
1347 manufacturing production under construction in America today.

1348 *Mr. Soto. So we saw what telecommunications -- we had
1349 to rip and replace because it was already in there, right?
1350 It was already too late, and we had to pull all this Huawei
1351 equipment back. Is there any other sort of economic
1352 development aspects we could help you with to boost
1353 production beyond sort of stopping the dumping of Chinese
1354 robotics and drones?

1355 *Mr. Robbins. Yes, that is a great question,
1356 Congressman, and you are absolutely right. The GUARD Act is
1357 a defensive mechanism, and we need some offense, as well.

1358 What China does really well is they both support the
1359 companies that are manufacturing the robots, but they also
1360 support the companies that are acquiring the robots
1361 domestically in China. They create demand. So the Federal
1362 Government can be a better customer, first and foremost, in

1363 national labs, on military bases and other places, but also
1364 can create incentives for U.S. manufacturing to purchase
1365 American-made robots and install them in the factories.

1366 We have about -- over a 500,000 manufacturing job
1367 shortfall in America right now, and American robotics can
1368 help enhance American manufacturing efficiency and U.S. GDP
1369 by helping to enhance manufacturing efficiency.

1370 *Mr. Soto. Thank you, and I yield back.

1371 *Mr. Robbins. Thank you, sir.

1372 *Mr. Hudson. [Presiding.] Thank you. The chair now
1373 recognizes the gentleman from Ohio, Mr. Latta, for five
1374 minutes.

1375 *Mr. Latta. Well, thanks, Mr. Chairman, and thanks to
1376 our witnesses for being with us today. This hearing is very,
1377 very important.

1378 And if I could start with you, Mr. Van Ah, just -- I
1379 have been on this subcommittee for a good number of years and
1380 chaired it. But, you know, when we talk about having 130
1381 broadband programs across 15 different departments and
1382 agencies, and we -- the question always comes up, how much --
1383 you know, how many do we really need? We don't need that
1384 many. I know we don't.

1385 And the question, I guess, has GAO done a report as to
1386 the cost of having that many different programs across that
1387 many departments and agencies?

1388 *Mr. Von Ah. We haven't delved into the costs in terms
1389 of whether there is sort of, like, you know, a duplicative
1390 effort across the agencies. We haven't honed in on the exact
1391 cost of that. But certainly, there is overhead in each
1392 agency to execute those programs. So if you have got sort of
1393 repetitive and duplicative overhead in those --

1394 *Mr. Latta. Well, let me ask, is that something then
1395 this committee, the subcommittee, could ask of you at GAO, to
1396 do a cost estimate on that?

1397 *Mr. Von Ah. Well, we could certainly discuss that,
1398 certainly, with your staff.

1399 *Mr. Latta. Okay. Well, thank you.

1400 Ms. Gorman, if I could ask a quick question for you
1401 because -- so short on time when we only have five minutes
1402 and so many questions -- in the last bullet point in your
1403 testimony you have "rebuild tech trust with U.S. allies and
1404 partners'", and you talk about, you know, about the U.S.
1405 leadership that has been out there, and that we need to be
1406 back out in front.

1407 But we have also been talking about Huawei and ZTE, and
1408 we did a \$4.8 billion rip-and-replace in this country because
1409 they are not a trusted network. And we know that these -- a
1410 lot of countries out there get it because it is "cheap'".
1411 But, you know, you -- sometimes you end up selling your soul
1412 to get the -- get what Huawei and ZTE is giving. How do we

1413 regain that trust, when -- because -- when everybody knows
1414 this is not trusted equipment that the Chinese are putting
1415 out there?

1416 *Ms. Gorman. I very much agree. And in fact, I think
1417 we -- for our allies and partners, we should be continuously
1418 pointing out the risks not just to us, not just to someone
1419 else, but actually to them of using these vendors. The
1420 intellectual property theft, the displacement of their own
1421 industries that are at risk.

1422 I think some countries, you know, also -- and some
1423 parts, particularly in Europe, look at the U.S. and say,
1424 well, we want to move towards our own sovereign approaches.
1425 And I think that would be much more difficult than if we come
1426 up with an allied strategic approach, where we can use
1427 trusted vendors across our allies and partners. And so that
1428 is the kind of trust in the United States, in our ecosystem
1429 of allies and partners that I think is critical to ensuring
1430 that we don't make choices in this country and in our closest
1431 allies and partners about using some of these untrusted
1432 vendors like Huawei and ZTE.

1433 *Mr. Latta. Thank you.

1434 Mr. Robbins, you know, you have talked about the --
1435 especially in your testimony -- that 96 percent of the
1436 uncrewed aircraft in the United States is coming from one
1437 source, from the PRC. And that is truly unacceptable. I

1438 know we have been trying to get something done about that.

1439 But we all know the absolute risk of having these drones
1440 flying around the United States, collecting information on
1441 us. Law enforcement has said, oh, we really like the
1442 technology. And we -- how do we say that, you know, folks,
1443 it might be time to turn those things off, put them in the
1444 closet, and leave them there? Has there been a lot of
1445 discussion out there to tell people that they better not be
1446 using -- because I know when I am out and I am asked I say,
1447 don't use them.

1448 *Mr. Robbins. Yes, I appreciate that, Congressman. And
1449 I think the conversation has evolved a lot. The education
1450 work done by Congress, by agencies like CISA and the FBI have
1451 really put out a lot of good information on the risk of using
1452 Chinese drones and the national security implications of
1453 that.

1454 But we also have to recognize that, you know, local law
1455 enforcement, public safety agencies, they typically have
1456 very, very tight budgets. And they have made, in some cases,
1457 very significant investments in their Chinese drone fleets.
1458 And it is not an easy switch for them to just turn those off
1459 and go back to not having drones because they are a
1460 lifesaving tool. It is also not easy for them to go out and
1461 -- into the market and find new dollars to buy replacement
1462 drones.

1463 Congress did have a rip-and-replace program, as we
1464 talked about, for the telecommunication network when there
1465 was a clear national security risk with ZTE and Huawei. We
1466 would very much like to see a similar rip-and-replace program
1467 for drones. There are a few grant programs out there now
1468 that are helping communities -- DoJ grants, DHS grants, FEMA
1469 grants -- acquire non-Chinese drone technology as the Chinese
1470 drone technology is being faded out because of the FCC
1471 ruling. But it is not a lot of money right now, and that is
1472 certainly an opportunity for Congress to step in and help
1473 local public safety agencies make this transition faster.

1474 *Mr. Latta. Well, thank you very much. My time is
1475 expired, and I will submit questions that I didn't have time
1476 to ask to the witnesses.

1477 [The information follows:]

1478

1479 *****COMMITTEE INSERT*****

1480

1481 *Mr. Latta. Thank you very much, Mr. Chairman, I yield
1482 back.

1483 *Mr. Hudson. Thank you. The chair now recognizes the
1484 gentleman from California, Mr. Peters, for five minutes for
1485 your questions.

1486 *Mr. Peters. Thank you, Mr. Chairman. Thanks for
1487 calling this important hearing.

1488 We have discussed many times on this subcommittee just
1489 how critical broadband connectivity is in our increasingly
1490 online world. And in an age of technology, it is more
1491 important than ever for my constituents in San Diego and
1492 Americans across the country to get connected as quickly as
1493 possible so they can access employment opportunities,
1494 education, telehealth care, and more.

1495 In 2022 the Government Accounting [sic] Office, or GAO,
1496 released a broadband study on the "national strategy needed
1497 to guide Federal efforts to reduce the digital divide''. In
1498 this study GAO identified the over 130 Federal programs to
1499 expand broadband access administered by 15 different Federal
1500 agencies. The amount of investment shows that the Federal
1501 Government truly understands the importance of connectivity.
1502 However, the study found that this vast number of programs
1503 spread across so many agencies has led to a fragmented,
1504 confusing, overlapping patchwork of funding. I am concerned
1505 that the communities with the most limited resources may be

1506 the most affected by this fragmentation.

1507 Following the publication of the GAO report I introduced
1508 the PLAN for Broadband Act with my colleague, Representative
1509 Walberg. The PLAN for Broadband Act directly mirrors GAO's
1510 recommendation in this study to synchronize Federal efforts
1511 with the National Broadband Strategy.

1512 Mr. Von Ah, what is at stake with regards to this
1513 Federal program fragmentation?

1514 And which communities do you think are being harmed
1515 most?

1516 *Mr. Von Ah. Thank you for the question, Representative
1517 Peters.

1518 So going forward, right now there is, you know -- all
1519 these programs are underway in terms of trying to build out
1520 their broadband projects. And so what is key now is sort of
1521 what areas might be missed after those projects are
1522 completed. You know, will we get all of the areas covered
1523 that we want to have covered? Will there be sufficient
1524 coverage? Are there going to be those -- some carriers who
1525 drop out of these programs or default on their requirements,
1526 or their -- what they have promised to do, you know, over
1527 these programs?

1528 And then it is sort of what do we do at that point, and
1529 that is kind of where we are at this point. So in terms of
1530 the 130 programs, it has really boiled down to about a dozen

1531 programs or so that are focused on broadband deployment
1532 currently.

1533 *Mr. Peters. Yes.

1534 *Mr. Von Ah. And they are all underway.

1535 *Mr. Peters. All right. So you are not particularly
1536 concerned about the fragmentation? Or is there something you
1537 recommend we do about that?

1538 *Mr. Von Ah. I am still concerned about the
1539 fragmentation, of course. And I -- and what we have
1540 recommended to agencies is the importance of interagency
1541 collaboration on knowing what each agency is doing, where
1542 they are deploying broadband, whether they are trying to
1543 leverage those resources to basically bring communities up to
1544 speed.

1545 *Mr. Peters. Okay. Well, I am happy to see the PLAN
1546 for Broadband Act included in today's hearing after it was
1547 reported out of the Senate Commerce Committee last spring,
1548 and hope this bipartisan proposal -- we can see it through
1549 the committee to the floor soon.

1550 Today we are also discussing legislation to crack down
1551 on robocalls. There has been a lot of discussion about that.
1552 I consistently hear from my constituents about the harm
1553 robocalls cause. And just recently I heard from a senior
1554 citizen who resorted to changing his phone number to stop the
1555 approximately 20 scam calls he receives every single day.

1556 For many people, phone calls are the only way to stay in
1557 touch with loved ones or to receive important medical
1558 information. But thanks to the constant flood of scam
1559 robocalls, answering the phone can feel like taking a gamble,
1560 as if the scammers have taken over the whole system. So, Mr.
1561 Rupy, can you talk about how AI is changing the landscape for
1562 robocall scammers, and how we can, as Congress, can best
1563 protect our constituents from the scams that are becoming
1564 increasingly convincing?

1565 *Mr. Rupy. Thank you, Congressman, and yes, you know,
1566 it is an evolving landscape, and AI is certainly a tool that
1567 the scammers are using to make their fraud schemes seem more
1568 authentic, make them more convincing. And at the same time,
1569 like, those same tools are being used by industry to
1570 counteract those.

1571 There are challenges at times with -- you know, in the
1572 example you gave, you know, certain networks. IP networks
1573 versus TDM networks may be more capable of handling some of
1574 these tools. But at the end of the day, you know, industry
1575 is doing everything they can to, you know, deploy these
1576 tools, deploy AI to counteract these. But it is an ongoing
1577 process and I do believe that, you know, a criminal
1578 enforcement element is needed.

1579 *Mr. Peters. Okay, you mentioned that. That is
1580 something, obviously, we could add here.

1581 Thank you all for your testimony. I am glad to see the
1582 committee responding to these threats.

1583 And Mr. Chairman, I will yield back.

1584 *Mr. Hudson. Thank you. The chair now recognizes the
1585 gentleman from Virginia, Mr. Griffith, for five minutes for
1586 your questions.

1587 *Mr. Griffith. Thank you, Mr. Chairman.

1588 I appreciate -- Mr. Rupy, I appreciate your testimony.
1589 And I have gotten one -- I am not as popular as the chairman
1590 -- I have only gotten one spam call while we have been
1591 sitting here. And I am curious, though, because my
1592 constituents get these all the time too, but they -- a lot of
1593 them in my district and the complaints I get are people
1594 calling up on Medicare and Medicare Advantage-type programs.
1595 But like the chairman, I don't get those. Now, he is too
1596 young to get them, but I don't get those. I get the ones
1597 that want to lend me money. So how do they -- how -- what
1598 algorithm are they using to decide to call based on lending
1599 money or Medicare Advantage?

1600 *Mr. Rupy. Often times -- and thank you for that
1601 question, Congressman -- often times these scams -- they
1602 obviously vary, they come in different flavors. But often
1603 times the scammers will gain access to what are called lead
1604 lists, where, you know, because of something -- whether it is
1605 a cyber hack where that information was obtained, where they

1606 can find identifiable information about that particular
1607 consumer. You know, they are on Medicare, they are on
1608 Medicaid, they --

1609 *Mr. Griffith. They need to borrow money?

1610 *Mr. Rupy. They need to borrow money.

1611 [Laughter.]

1612 *Mr. Griffith. You know, that gets sold on the internet
1613 as a full package lead list, and they will start making those
1614 calls.

1615 And it can fluctuate. I used to get a lot of robocalls.
1616 And even though I answer them, fewer now it seems to me. But
1617 to your point, it is a very dynamic space and there is access
1618 to information that enables them to target individuals.

1619 *Mr. Griffith. And then I love the ones -- and I don't
1620 know whether anybody else has gotten these -- but I love the
1621 ones that where it says I am calling myself. I get a call
1622 from me.

1623 *Mr. Rupy. Where your --

1624 *Mr. Griffith. I am --

1625 *Mr. Rupy. -- phone number --

1626 *Mr. Griffith. It is my phone number that is calling me
1627 to tell me about whatever it is they want to sell me, yes.

1628 *Mr. Rupy. Right, and that is -- they are spoofing your
1629 caller ID.

1630 *Mr. Griffith. Right.

1631 *Mr. Rupy. Exactly.

1632 *Mr. Griffith. And I am -- I know that has happened to
1633 constituents, because they have told me that.

1634 So we are hearing all these complaints, and I am glad we
1635 are holding the hearing today to talk about H.R. 6152 which I
1636 am a cosponsor of. But it seems to me that you got these
1637 organized scam rings that are operating overseas to do this.
1638 And isn't that what the FCC Robocall Mitigation Database is
1639 supposed to block?

1640 And how come it isn't working, and how is it supposed to
1641 work?

1642 *Mr. Rupy. So I will say this. I think the FCC's
1643 robocall mitigation database plays a very important role.
1644 And, you know, at a very high level, the way it functions, if
1645 you are not in the database no provider can accept your
1646 traffic, right? So if a provider tries to go to, say,
1647 Verizon or AT&T, and Verizon and AT&T sees they are not in
1648 the database, they can't send or originate calls.

1649 I think the biggest challenge with the FCC's RMD is the
1650 quality of many of the entries. There are just fraudulent
1651 organizations, VoIP providers that are registered in the
1652 database. And the FCC, to its credit, has thrown -- done a
1653 lot to throw these providers out. They have removed about
1654 1,400 providers last year from the RMD. But I think, you
1655 know, the big issue is we need to catch them on the front end

1656 before they get in the database because, once they are in the
1657 database, they can make phone calls.

1658 *Mr. Griffith. And does the Foreign Robocall
1659 Elimination Act incentivize tracking down the bad actors?

1660 *Mr. Rupy. I believe it does, Congressman. And, you
1661 know, I think there is a lot of good things in the bill.
1662 Among other things, the task force that is formed. I am a
1663 big believer that, you know, good data informs good policy.
1664 And the task force strives to do that.

1665 On the traceback front, I think it is a great idea that
1666 we are moving that renewal process from one year to three,
1667 because all that is is a paperwork exercise for FCC
1668 Enforcement Bureau staff and the Traceback Consortium. So
1669 let's reduce the paperwork so they can focus on enforcement
1670 and traceback.

1671 And I do acknowledge that, you know, the RMD has a lot
1672 of issues and, you know, that is something that just today
1673 the FCC adopted a rulemaking on. They have initiated a
1674 rulemaking proceeding to see how best to tighten up the RMD.

1675 *Mr. Griffith. All right, and I appreciate it.

1676 I yield back, Mr. Chairman. I probably have questions
1677 for the record. Thank you.

1678 [The information follows:]

1679

1680 *****COMMITTEE INSERT*****

1681

1682 *Mr. Hudson. Thank you. The chair now recognizes the
1683 representative from Illinois, Representative Kelly, for five
1684 minutes for your questions.

1685 *Ms. Kelly. Thank you, Mr. Chairman and Ranking Member,
1686 for holding today's hearing. And thank you to our witnesses
1687 for being here.

1688 Reliable broadband is essential infrastructure. It
1689 connects families to health care, students to educational
1690 opportunities, and small businesses to customers around the
1691 world. It is critical to the success of American farmers and
1692 rural communities who increasingly rely on precision
1693 agriculture and other connected technologies to remain
1694 competitive.

1695 As the proud Democratic co-lead of the bipartisan Data
1696 BRIDGE Act, I believe one of the most important steps we can
1697 take to ensure that we are making decisions based on
1698 accurate, complete data [sic]. If our maps fail to identify
1699 agricultural areas, we risk overlooking farmers who depend on
1700 reliable connectivity to support food production and drive
1701 innovation. This legislation simply gives policy-makers
1702 better information by incorporating USDA-cultivated land maps
1703 into broadband maps so that broadband investments can be
1704 targeted where they are needed most.

1705 Improvements to the National Broadband Map will lead to
1706 better decisions, better stewardship of taxpayer dollars, and

1707 ultimately better outcomes for rural America.

1708 Mr. Von Ah, can you explain why incorporating
1709 agricultural land into FCC's broadband maps would improve
1710 Federal broadband planning and deployment decisions?

1711 *Mr. Von Ah. Absolutely. Thank you for that question,
1712 Representative Kelly.

1713 Our work over the last several years has continuously
1714 shown that the better, accurate -- more accurate data we have
1715 in maps, the better we can target our investments. That has
1716 been true going back to when FCC used census blocks to sort
1717 of identify where broadband was or wasn't. The more refined
1718 and more accurate data that we can get, the better we can
1719 target those investments.

1720 *Ms. Kelly. Thank you. And as farms increasingly rely
1721 on precision agriculture, connected equipment, and real-time
1722 data, what are the potential consequences to Federal
1723 broadband funding if these agricultural areas continue to be
1724 under-represented in our mapping efforts?

1725 *Mr. Von Ah. I think the answer is fairly simple, that
1726 they may not get the investment necessary to support those
1727 kinds of activities.

1728 *Ms. Kelly. And that affects our farmers and economic
1729 development. My district is urban, suburban, and rural, and
1730 I have 4,500 farms in my district. So they are definitely
1731 very interested in this.

1732 Well, thank you, and we must ensure greater access to
1733 broadband for all Americans, and that includes our farmers
1734 and rural communities who feel left out far too often.

1735 Thank you, and I yield back.

1736 *Mr. Hudson. Thank you. The chair now recognizes the
1737 representative from Texas, Representative Pfluger, for five
1738 minutes for your questions.

1739 *Mr. Pfluger. Yes, thank you, Chairman, and thanks for
1740 holding this hearing.

1741 And to our witnesses, we appreciate your testimony as we
1742 look through these issues. Every phone call, every text and
1743 transaction that Americans make travel across networks that
1744 are under growing attack, and I think we can -- you all have
1745 mentioned that today.

1746 But recent reporting showed millions of attacks launched
1747 against U.S. telecom providers in a single year, and those --
1748 that obviously has a cost that is associated with it --
1749 billions of dollars, in fact. And AI has given our
1750 adversaries a powerful new tool to launch these attacks at a
1751 scale that we have not seen maybe ever.

1752 And it should also be one of our best tools to stop
1753 them, AI should be that tool that we can help leverage and
1754 stop, and I think that is important and that is why
1755 Congressman Menendez and I introduced the bipartisan AI for
1756 Secure Networks Act, which directs the Department of Commerce

1757 to examine how AI can be responsibly used to strengthen the
1758 security and resilience of telecommunications networks.

1759 So Ms. Gorman, I will start with you. You have said
1760 that AI risks tipping the offense-defense balance in the
1761 attacker's favor, even as it shows real promise for automated
1762 threat detection. Can you maybe expand a little bit on where
1763 is AI-based network defense mature enough to deploy right
1764 now?

1765 And then, on the other side of that coin, where does it
1766 still need to grow?

1767 *Ms. Gorman. Yes, thank you, Congressman, for the
1768 question.

1769 And I think this is -- the offense-defense battle
1770 balance is evolving. These technologies are evolving so
1771 rapidly that every week there is a new development. But I
1772 agree, and I agree with the premise of the AI for Secure
1773 Networks Act, that we need to be leveraging these
1774 technologies for defense.

1775 Where I think these technologies are increasingly mature
1776 is in finding vulnerabilities that we might not be able to
1777 find with other means. That is incredibly powerful for both
1778 attackers and, of course, also for defenders.

1779 Where I think there is still work to be done is exactly
1780 in this question of what kinds of models and what
1781 cybersecurity standards of the models themselves are we going

1782 to allow into our networks to monitor the traffic on
1783 networks, to find vulnerabilities, to monitor for suspicious
1784 behavior. Right now we don't have any requirements on
1785 cybersecurity standards of the models themselves. They are
1786 subject to data poisoning, they are subject to prompt
1787 injection attacks. They could be using adversarial models.
1788 So I think that is really the biggest barrier to fully
1789 integrating these AI models into network defense.

1790 *Mr. Pfluger. Thank you.

1791 Mr. Robbins, you have made the case that the connected
1792 sensor-rich devices pose a risk, whether the robots are a
1793 network or equipment or otherwise, and I agree with that.
1794 Does the same logic apply to how we think about deploying AI-
1795 enabled monitoring tools across telecom networks?

1796 *Mr. Robbins. Yes, thank you for that question,
1797 Congressman.

1798 We see robots as the physical manifestation of AI. It
1799 is embodied AI. So yes, that logic absolutely is sound.

1800 *Mr. Pfluger. I want to talk robocalls, and I know that
1801 this has been discussed, but it is obviously one of the top
1802 complaints that we hear, and -- assuming that most of my
1803 colleagues are also getting the same.

1804 But according to the FCC, illegal and spoofed robocalls
1805 remain its top consumer protection priority, and a large
1806 share of that traffic is originating in foreign locations

1807 with foreign-based robocallers. And it is a huge problem and
1808 a challenge.

1809 The TRACED Act, signed into law in 2019, directed the
1810 FCC to designate a single consortium to run private-lead
1811 traceback efforts, and they have redesignated the Industry
1812 Traceback Group every year since 2020. Mr. Rupy, you helped
1813 build the ITG from scratch. And how would extending that
1814 consortium's designation from one year to three years, say,
1815 affect its ability to actually go after robocallers and have
1816 a higher effective rate?

1817 *Mr. Rupy. Thank you, Congressman. I think that
1818 extension makes great sense, and, you know, the main reasons
1819 are I think it is prudent that the TRACED Act established a
1820 review period for the designated Traceback Consortium, but it
1821 is sort of a Goldilocks scenario, right? Like, one year is a
1822 little too short, three years is an ideal period because each
1823 and every year the FCC has to go through an administrative
1824 process. If a competing application is filed, the Traceback
1825 Consortium has to respond.

1826 So in my mind, it is a more efficient process that
1827 enables both the Enforcement Bureau and the Traceback
1828 Consortium to do what they do best, which is find bad guys
1829 and target them.

1830 *Mr. Pfluger. Thank you. Five minutes is hard to get
1831 everything solved, but I appreciate that.

1832 I yield back, Chairman.

1833 *Mr. Hudson. Thank you. The chair now recognizes the
1834 representative from California, Representative Barragan, for
1835 five minutes for her questions.

1836 *Ms. Barragan. Thank you, Mr. Chairman.

1837 Last year seniors lost \$7.7 billion to scammers, up to
1838 59 percent from the year before, and part of that came from
1839 what the FBI calls the distress scams, where the AI voice
1840 cloning tools mimic a grandchild's voice to fake an
1841 emergency.

1842 Mr. Rupy, these scams are already happening today. In
1843 addition to the QUIET Act, what else can Congress do to stop
1844 that call before it ever reaches someone?

1845 *Mr. Rupy. Thank you, Congresswoman, and, you know, I
1846 don't want to sound like a broken record, but I do believe
1847 that, you know, in my mind, we can find the individuals
1848 originating these calls. We can find them, we can locate
1849 them, and we can find the organizations that are, you know,
1850 managing that process.

1851 And that is a heartbreaking scam. It is terrible. My
1852 own 90-year-old mother received a call like that. But that
1853 is why I really think we need to start focusing on criminal
1854 enforcement. I think too often people think about robocalls
1855 as a nuisance, a bother. It is no longer that. This is --
1856 you know, as I noted in my opening testimony, it is not only

1857 a major consumer harm issue, it is national security.

1858 *Ms. Barragan. Is there anything in the current law now
1859 that would stop the call before it connects?

1860 *Mr. Rupy. I think the closest thing that would stop a
1861 call before it connects is removal from the FCC's Robocall
1862 Mitigation Database.

1863 In other words, you know, whoever that provider is that
1864 is originating those calls, once they are taken out of the
1865 database, they can't do that anymore. And the FCC has done
1866 that. They have, you know, removed 1,400 last year from the
1867 RMD.

1868 *Ms. Barragan. Thank you. One more on this is a lot of
1869 my constituents speak Spanish or another language at home
1870 first. And scam operations already run calls in multiple
1871 languages. Does a disclosure rule like the QUIET Act protect
1872 someone if the scam isn't happening in English, or are non-
1873 English speakers more exposed and less protected than
1874 everyone else?

1875 *Mr. Rupy. Thank you, Congresswoman.

1876 In my opinion, I don't think that imposing compliance
1877 mandates will lower the prevalence of those calls or reduce
1878 those calls because, at the end of the day, the bad actors
1879 behind those calls, they don't care about compliance. They
1880 don't observe do-not-call mandates, they do not disclose
1881 their actual identities. And, you know, it is not going to

1882 have the downward pressure on illegal robocalls that we all
1883 want, in my opinion.

1884 *Ms. Barragan. Is there any kind of tracking of whether
1885 these scams are -- disproportionately target non-English
1886 speakers, or is that data we don't have?

1887 *Mr. Rupy. There are certainly vendors out there and,
1888 you know, potentially some carriers that have that
1889 information. They can see where these scams are occurring
1890 geographically. So companies like YouMail, Nomorobo, and
1891 others, they can see that data.

1892 *Ms. Barragan. Great, thanks.

1893 Mr. Von Ah, a 2023 report that you authored found that
1894 nearly a third of families without broadband said the reason
1895 was cost, and a quarter of families who already had it
1896 struggled to afford it. Now, those same families are paying
1897 up to \$30 or more -- \$30 a month more, which is almost \$350 a
1898 year since the Affordable Connectivity Program ended. Does
1899 GAO still consider the single biggest barrier between
1900 families -- does it -- does GAO still consider cost the
1901 single biggest barrier between families and affordable
1902 broadband?

1903 *Mr. Von Ah. If it -- it is certainly one of the key
1904 issues, if not the most critical one, yes.

1905 *Ms. Barragan. It is not the most critical? Cost is
1906 not the most critical?

1907 *Mr. Von Ah. No, it certainly is one of the most
1908 critical, yes.

1909 *Ms. Barragan. Oh, it is one of the most critical.
1910 Because I saw a report the GAO had, and it mentioned a number
1911 of programs that were important, and that -- the Affordable
1912 Connectivity Program was one of them.

1913 *Mr. Von Ah. Right.

1914 *Ms. Barragan. Do you think that helped people afford
1915 access to broadband?

1916 *Mr. Von Ah. While that program was going on, it --
1917 there were some 24, 23 million subscribers to that program
1918 that benefitted from that particular program.

1919 After it was -- after it ran out of money, I think the
1920 sort of -- estimates that some five million or so subscribers
1921 discontinued their service and some eight million more
1922 perhaps, you know, would -- either downgraded their service
1923 or went to try to find some lower-cost options. So --

1924 *Ms. Barragan. So millions of people lost access to
1925 broadband when that program went away.

1926 *Mr. Von Ah. Some did lose access to broadband. And
1927 then, I -- what we understand more recently is that they are
1928 trying to find ways to get broadband back.

1929 *Ms. Barragan. Yes.

1930 *Mr. Von Ah. So they are trying to find, you know,
1931 cheaper, lower-cost options.

1932 *Ms. Barragan. Well, they need Democrats back in power
1933 to do that.

1934 I yield back.

1935 *Mr. Hudson. The chair recognizes the gentleman from
1936 Louisiana, Mr. Carter, for five minutes for your questions.

1937 *Mr. Carter of Louisiana. Thank you, Mr. Chairman, and
1938 I thank the witnesses for being here. We appreciate your
1939 time and expertise.

1940 Broadband is the critical infrastructure that connects
1941 our communities and enables people to fully participate in
1942 the modern economy. It powers nearly every sector of our
1943 society. And as artificial intelligence continues to evolve,
1944 reliable high-speed connectivity will not only become more
1945 essential, but will be more needed in areas than ever before.

1946 If the United States wants to remain a global leader in
1947 innovation and compete with other nations, we cannot afford
1948 to leave people behind because the lack of reliable
1949 connectivity. That is why the Broadband Equity Access and
1950 Deployment, or BEAD, program is so important. This historic
1951 investment was intended to fully -- to finally connect rural
1952 and underserved communities to high-speed internet.

1953 Unnecessary deployment delays only widen the digital
1954 divide and postpone economic opportunity. We know that
1955 broadband is the backbone of telehealth. It allows patients,
1956 especially in rural areas, to access quality health care

1957 without traveling long distances. But without reliable
1958 infrastructure, broadband infrastructure, telehealth simply
1959 is not an option for those who need it most. As our
1960 technology continues to evolve, we must continue investing in
1961 communication technology and networks to connect everyone,
1962 regardless of their zip code.

1963 Mr. [sic] Gorman, why is resilient broadband
1964 infrastructure an essential component for consumers to fully
1965 leverage artificial intelligence?

1966 *Ms. Gorman. Thanks for the question. I think a few
1967 reasons.

1968 First, that throughout -- we are in a global competition
1969 to develop AI, to deploy AI, and we need the best and
1970 brightest from this country to be part of that race and that
1971 contest. And right now, if students around the country are
1972 unable to access artificial intelligence, are unable to build
1973 their own tools because of lack of access to broadband, we
1974 may not get the best and the brightest as part of this
1975 geopolitical competition.

1976 Additionally, you mentioned the rural and underserved
1977 communities, telehealth. I actually think some of the most
1978 innovative applications of artificial intelligence are
1979 exactly in these fields. Taking a global example in India,
1980 AI helped farmers massively increase yields, productivity,
1981 decrease the amount of pests in crops. I think we can do the

1982 same thing in many, many farming communities across the
1983 United States.

1984 And similarly, telehealth is an area where -- throughout
1985 the country I think we have all had the experience of being
1986 plagued by wait times, high costs. And there is real room
1987 for AI disruption and innovation, and I agree that that is
1988 only possible with connectivity and broadband throughout.

1989 *Mr. Carter of Louisiana. Thank you.

1990 Mr. Van Ah, how can communities be harmed when high-
1991 speed, reliable internet isn't available, especially when it
1992 comes to health care outcomes?

1993 *Mr. Von Ah. Well, thank you for the question,
1994 Representative Carter.

1995 I mean, in general they forgo the benefits of being able
1996 to participate in the internet economy, right, which could
1997 mean things like job opportunities or business opportunities.
1998 It could --

1999 *Mr. Carter of Louisiana. When health care clinics are
2000 closing down because of drastic cuts to Medicaid, and we are
2001 seeing clinics and critical care units going away and, in
2002 some cases, rural hospitals, the only access they have will
2003 be through telehealth.

2004 *Mr. Von Ah. Right. And so they would also forego the
2005 benefits of, you know, opportunities or information available
2006 on their -- from -- in the health care setting, for sure, as

2007 well.

2008 *Mr. Carter of Louisiana. Mr. Rupy, you indicated that
2009 we know where the bad actors are, those who are perpetuating
2010 these erroneous phone calls that are scamming, telling the
2011 chairman that he has got \$45,000 waiting to just pick up, or
2012 calling to say we would like to buy a property that you own,
2013 or calling to say that I am stuck in -- on some foreign
2014 island and I lost my credentials, and I need \$1,000 just to
2015 get home. These happen all the time.

2016 Our aged communities are finding themselves more and
2017 more vulnerable to these bad actors who call with what
2018 appears to be legitimate phone calls with people with
2019 distress. You indicated that we could find them. How
2020 successful are we in actually finding them and bringing them
2021 to justice?

2022 *Mr. Rupy. Well, I think we are very successful at
2023 identifying these parties.

2024 I mean, it -- the way traceback works, the traceback
2025 goes from the point of termination to who made the call. I
2026 think the challenge we have here is, you know, the will to go
2027 to that next step to pursue meaningful enforcement actions.

2028 You know, the FCC and the FTC and state AGs have
2029 undertaken a number of civil enforcement actions. But again,
2030 I think, you know, in that instance you are talking about I
2031 -- you know, I believe that we need criminal enforcement

2032 action.

2033 *Mr. Carter of Louisiana. I have got a ton of more
2034 questions, but my time is exhausted. So Mr. Chairman, I
2035 yield.

2036 *Mr. Hudson. I thank the gentleman. The chair now
2037 recognizes the representative from Indiana, Representative
2038 Houchin.

2039 *Mrs. Houchin. Sorry, Mr. Menendez.

2040 Thank you, Mr. Chairman and Ranking Member Matsui, for
2041 holding this hearing. And thank you to the witnesses.

2042 Two things on today's agenda matter a great deal to the
2043 people back home in Indiana: getting reliable internet
2044 service to the places that still don't have it, and stopping
2045 a flood of scam calls from hitting their phones.

2046 On scam calls, this is one of the biggest issues I hear
2047 about from constituents. They are getting them every day,
2048 sometimes all day, every day. And the people running these
2049 are increasingly organized criminal operations overseas. I
2050 appreciate the work that my colleagues have done on the
2051 Foreign Robocall Elimination Act as well as the QUIET Act,
2052 and I look forward to seeing more activity on this topic.
2053 Lord knows, we could all use quieter phones, less scam texts,
2054 and less scam calls.

2055 But on broadband, I am pleased to see that H.R. 4950,
2056 the Data BRIDGE Act, is included in today's hearing. I want

2057 to thank my colleague, Ms. Kelly, for co-leading the bill
2058 with me, and Mr. Soto and Mr. Landsman for their support as
2059 cosponsors.

2060 The FCC keeps a National Broadband Map that shows where
2061 internet service is available, and the Federal Government
2062 uses it to decide where to send broadband funding. But the
2063 map is built around homes and businesses; it does not show
2064 farmland. That is a problem because farming today runs on
2065 connectivity out in the field: on guidance systems, sensors,
2066 monitors, and equipment that has to talk to a network. A
2067 farm can be counted as covered on the traditional broadband
2068 map at the farmhouse, while the acres where the actual work
2069 happens have no service. The Data BRIDGE Act aims to solve
2070 that problem by directing the FCC to place data that the USDA
2071 already collects on the broadband map -- onto the broadband
2072 map. Right now the FCC has a map showing where service is
2073 available. There is a separate Federal map showing where
2074 agencies are funding deployment.

2075 Mr. Von Ah, is it fair to say that improving the
2076 broadband maps is one of the highest-return, lowest-cost
2077 things Congress can do to address broadband deployment?

2078 *Mr. Von Ah. Thank you for that question. It is --
2079 certainly improving the accuracy of the maps goes a long way
2080 to better targeting Federal investment.

2081 *Mrs. Houchin. And it helps prevent us from over-

2082 building. It might also help us in these dead zones.
2083 According to the map it looks like they are covered, but they
2084 are actually dead zones. It might help us spur some Federal
2085 investment to finally get those, what we consider the final
2086 miles, covered with access. Is that correct?

2087 *Mr. Von Ah. That is correct.

2088 *Mrs. Houchin. Are the USDA, the NTIA, and Treasury
2089 sitting on their own data? Or are they submitting that data
2090 to the FCC for maps?

2091 *Mr. Von Ah. So the agencies have some agreements in
2092 place on the data they share about their deployments. We
2093 have made some recommendations about them agreeing to the
2094 timeframes and the kinds of data that they send to those maps
2095 because we see certainly a lag in those maps when a
2096 deployment has been made and whether it shows up on the map
2097 or when it shows up on a map.

2098 *Mrs. Houchin. So should the FCC's broadband map be the
2099 unified source of truth for Federal broadband decisions on
2100 these dollars?

2101 *Mr. Von Ah. At this point it is our best option,
2102 although there are -- and I think the agencies do refer to --
2103 other sources when they are coordinating to avoid duplicative
2104 effort.

2105 *Mrs. Houchin. Thank you. A principle that runs
2106 through the GAO's work is that agencies should use the data

2107 that the government has already collected before devising
2108 anything new. Is putting an existing Federal data set onto
2109 an existing Federal map exactly that principle in practice?

2110 *Mr. Von Ah. Yes. Our work would suggest that we want
2111 to make sure that the data that we add would be accurate,
2112 right? So we did notice in the legislation this notion that
2113 it would be developed in concert with agriculture data,
2114 existing data. And so that certainly is an important piece
2115 of it.

2116 *Mrs. Houchin. We don't have to reinvent the wheel.

2117 Do you see other opportunities where the data the
2118 Federal Government already holds could be useful in making
2119 the map more accurate?

2120 *Mr. Von Ah. We have recommendations, again, for the
2121 agencies to sort of continue to feed data to the map and to
2122 do it in a more uniform and timely manner. And so that is
2123 what we would like to see, yes.

2124 *Mrs. Houchin. Well, whether it is stopping scam calls
2125 or closing this digital divide, the through line today with
2126 this hearing is clear: the Federal Government works best
2127 when it is coordinated and working from good information.
2128 The Data BRIDGE Act delivers on that by providing a more
2129 complete broadband map built from the data the government
2130 already collects at no new cost. I urge my colleagues to
2131 support H.R. 4950 as it moves through the committee process.

2132 I thank the witnesses. Thank you, Mr. Von Ah.

2133 And I yield back.

2134 *Mr. Hudson. Thank you. The chair now recognizes the
2135 gentleman from New Jersey, Mr. Menendez, for your questions.

2136 *Mr. Menendez. Thank you, Mr. Chairman.

2137 Our district sits at the heart of America's critical
2138 infrastructure. The corridor between Newark Airport and the
2139 Port of Elizabeth has been called the most dangerous two
2140 miles in America because of the particular risk to our
2141 transportation, energy, communications, and commercial
2142 infrastructure. A disruption here wouldn't just affect New
2143 Jersey, it would have cascading consequences for communities
2144 and businesses across the country.

2145 For our community, secure and reliable communications
2146 networks are essential. They link families to emergency
2147 services, banks, hospitals, and schools, and ensure a quick,
2148 effective response in the event of an attack against our
2149 infrastructure. As cyber threats grow more sophisticated, we
2150 need the strongest tools available to defend these networks.

2151 AI can help providers protect our communities from
2152 disrupted communications networks. Used responsibly, AI can
2153 help identify vulnerabilities and respond to threats more
2154 quickly. But used maliciously, it can make cyber attacks
2155 more damaging and harder to stop. Congress has a
2156 responsibility to address both realities. That is why

2157 Congressman Pfluger and I introduced the bipartisan AI for
2158 Secure Networks Act. Our bill would promote the responsible
2159 use of AI to strengthen the cybersecurity of America's
2160 communications networks, while confronting the risks posed by
2161 its misuse.

2162 We cannot afford to stand by as threats to the networks
2163 American families rely on every day continue to grow in
2164 scale, sophistication, and severity. As cyber attacks become
2165 more frequent and sophisticated, Congress must act to protect
2166 these systems and the communities they serve.

2167 Ms. Gorman, just briefly, given the concentration of
2168 critical infrastructure in and around New Jersey, would you
2169 agree that a cyber attack on our networks could have far-
2170 reaching consequences for both our communities and the
2171 nation?

2172 *Ms. Gorman. They could be among the most disruptive
2173 attacks.

2174 *Mr. Menendez. I agree. Mr. Rupy, just briefly, how
2175 does AI-powered threat detection and response help prevent
2176 these attacks and protect the families, hospitals, first
2177 responders, and airports that depend on reliable
2178 communications networks?

2179 That was for you, Mr. Rupy.

2180 *Mr. Rupy. I think, as -- thank you, Congressman. I
2181 think, you know, communications companies are leveraging AI

2182 to protect the networks because, as you noted, adversaries
2183 are likewise deploying it. So it is a bit of an arms race.

2184 *Mr. Menendez. Yes, it is on both the offensive and
2185 defensive capabilities, and so being prepared for both.

2186 While AI offers opportunities for innovation and
2187 security, we also know that bad actors are also using this
2188 technology to exploit our vulnerabilities and improve cyber
2189 attack capabilities. Ms. Gorman, as bad actors increasingly
2190 use AI to launch more advanced attacks, how could the AI for
2191 Secure Networks Act help network providers and Federal
2192 agencies better understand and keep pace with these evolving
2193 risks?

2194 *Ms. Gorman. Thank you, Congressman, for the question.

2195 Generally, when such a breach happens, one of three
2196 things has occurred. Either a known vulnerability that was
2197 unpatched gets exploited, an unknown vulnerability gets
2198 exploited, or there was some kind of a human error. Someone
2199 clicked on a phishing link, someone had an insecure password.
2200 AI can be helpful with all three of these tools, and that --
2201 and all three of these types of exploits: finding
2202 vulnerabilities that we don't know about, automatically
2203 patching vulnerabilities that we should know about, and also
2204 flagging potential phishing attacks for the humans so we
2205 don't make those errors. That is why I think this -- the
2206 Secure Networks -- AI for Secure Networks bill can be so

2207 vital to figure out which are the threats that are actually
2208 coming from AI into our networks which are causing us the
2209 most harm, and what can we actually be deploying to combat
2210 that.

2211 And this technology is moving so quickly that this needs
2212 to be more than just a one-time thing. We need to be
2213 continuously updating our understanding, and I think this Act
2214 is a great start to provide this information across the
2215 Federal Government.

2216 *Mr. Menendez. I appreciate that, because American
2217 families should not have to worry that a cyber attack could
2218 cut them off from emergency services or the people they love.
2219 Our networks are too important, and the stakes are simply too
2220 high for Congress not to act. I am proud that this committee
2221 is advancing bipartisan solutions to strengthen these
2222 systems, protect families, and keep communities across the
2223 country connected.

2224 Thank you, Chairman, and I yield back.

2225 *Mr. Allen. [Presiding.] The gentleman yields. Now I
2226 call on Representative McClellan for your five minutes of
2227 questions.

2228 *Ms. McClellan. Thank you, Mr. Chairman.

2229 U.S. households have, on average, 21 devices connected
2230 to the internet, and I expect this is only going to grow as
2231 AI, robotics, and other smart Internet of Things devices

2232 become more integrated into our daily lives. This makes
2233 reliable and secure communication networks more important
2234 than ever.

2235 And at the same time, we have seen what happens when we
2236 do not act fast enough to address the growing cyber and
2237 national security threats early. We must learn from the past
2238 to inform the future. The stakes are too high to do
2239 otherwise, and that is why I am proud to work with Chairman
2240 Moolenaar on the bipartisan GUARD Act, which takes a
2241 proactive approach to evaluating the national security risks
2242 posed by connected robotics before those technologies become
2243 deeply embedded in our economy and critical infrastructure.

2244 And with that I want to start with you, Mr. Robbins. I
2245 think we can all agree that we should not repeat the mistakes
2246 that left the United States scrambling to remove Huawei and
2247 ZTE equipment only after it had already been become embedded
2248 in our communications networks and posed a significant
2249 national security risk. In your view, what makes the Covered
2250 List an effective national security tool?

2251 And are there other tools or authorities that Congress
2252 should consider to ensure that the U.S. maintains pace with
2253 China's rapid deployment of robotics?

2254 *Mr. Robbins. Yes, thank you for that question,
2255 Congresswoman, and thank you for your leadership on the GUARD
2256 Act. It is very much sincerely appreciated.

2257 So first of all, the Covered List is a good source of
2258 action with -- the GUARD Act directs the FCC to take action
2259 because the FCC has the authority to take care of this
2260 proactively. They can -- as they have done with drones and
2261 internet routers, restricted the import of future models,
2262 which doesn't necessarily impact the models that are already
2263 here. That ensures that there is a cut-off point, it gives
2264 investors certainty that the market is not going to continue
2265 to be flooded with subsidized Chinese robots or drones and
2266 further injecting national security risk into the United
2267 States.

2268 The FCC also has a lot of agility in their ability to
2269 act. So when a company takes an action, like sets up a fake
2270 subsidiary, a white label company to then continue to try and
2271 do operations in the United States, the FCC has the agility
2272 to quickly take action and ban that subsidiary. And in fact,
2273 they just did so this week with 9 or 10 fake companies that
2274 were operating as white label subsidiaries of a Chinese drone
2275 company, DJI.

2276 *Ms. McClellan. And what is the worst case scenario if
2277 we wait too long to confront the potential threats posed by
2278 Chinese-made communications equipment, technology, and
2279 services, and advanced robotics?

2280 *Mr. Robbins. Yes, the risk is that they become
2281 embedded in society like Chinese drones did. And then the

2282 cost of rolling that back is significantly greater to the
2283 American people while we are also exporting the data that the
2284 robots are collecting right back to China, powering their
2285 innovation, powering their research. You know, research
2286 labs, universities, they are doing research today primarily
2287 on artificial intelligence. With Chinese robots, all that
2288 data is going right back to China. We are handing this, a
2289 gift, to them. So, you know, their flooding the U.S. market
2290 with subsidized robots is strategic.

2291 *Ms. McClellan. And what is at stake for American
2292 start-ups and our robotics research and development ecosystem
2293 if Chinese-made robotic and communication technologies
2294 continue to undercut U.S. innovation?

2295 *Mr. Robbins. Yes, it is going to be very challenging
2296 for companies to be able to compete. I think U.S. innovation
2297 will continue to lead the world, but it is very challenging
2298 for companies to scale manufacturing. It is very hard for
2299 them to raise the money to hire the workforce and build out
2300 the floor plan when investors see what is happening in other
2301 industries, where China has come in, flooded the market, and
2302 drove companies either out of business or kept their market
2303 share small because they have artificially low prices.

2304 *Ms. McClellan. And so you would agree that it is
2305 important that Congress act now to ensure that American
2306 companies compete on a level playing field, and that the

2307 United States remains a global leader in these critical
2308 technologies?

2309 *Mr. Robbins. Absolutely. Congress should act now.

2310 *Ms. McClellan. Okay.

2311 *Mr. Robbins. That is right.

2312 *Ms. McClellan. And I may not have time to get an
2313 answer to this, so I will ask you all to respond in -- on the
2314 record.

2315 [The information follows:]

2316

2317 *****COMMITTEE INSERT*****

2318

2319 *Ms. McClellan. But, you know, Ms. Gorman, you have
2320 seen -- and I am sure we have talked about already -- the
2321 news that during the testing phase of OpenAI's GPT 5.6 and
2322 more powerful unreleased models, their ability to, you know,
2323 break out and go rogue. This is an unprecedented event in
2324 which AI acts outside of its directives and could become more
2325 commonplace. So what safeguards should we be looking at so
2326 that the very technology that we are using to protect our
2327 critical infrastructure works for us and not against us?

2328 *Ms. Gorman. I am happy to happy to answer more fully,
2329 but essentially, this is the question of model alignment.
2330 And making sure that we assess models for alignment before
2331 deploying them in critical infrastructure is vital.

2332 *Ms. McClellan. Thank you.

2333 I yield back.

2334 *Mr. Allen. The gentlelady yields, and now I call on
2335 Dr. Joyce for your five minutes of questioning.

2336 *Mr. Joyce. Thank you, Mr. Chairman, for allowing me to
2337 join in this important hearing.

2338 Bridging the digital divide and improving connectivity
2339 is a top priority for my constituents. Representing rural
2340 south central, and southwestern Pennsylvania, I am keenly
2341 aware of the unique challenges that rural agricultural
2342 communities face when it comes to getting connected.

2343 Rural communities consistently fall behind the rest of

2344 the country, seeing technology continue to advance. While
2345 many state and Federal programs exist to help bridge this
2346 gap, that divide is still very wide. These communities are
2347 strong, they are hard-working, they contribute to our nation.
2348 And without them we wouldn't have food on our tables tonight
2349 for dinner. They deserve our unwavering support.

2350 This subcommittee has done extensive work in examining
2351 the unique roles and needs of our rural communities, and
2352 diligently working to solve these problems. But there is
2353 still work to be done, and there is still broadband to
2354 deploy. Having reliable data to drive that deployment is
2355 necessary as we seek to ensure universal broadband
2356 availability for each and every American.

2357 Accurate broadband mapping is critical to the efficient
2358 use of taxpayer dollars for the administration of Federal
2359 broadband programs that aim to deliver necessary
2360 telecommunications infrastructure to rural communities. Mr.
2361 Von Ah, current data can sometimes be unreliable. I think we
2362 can agree on that. Can you speak about your recommendations
2363 for improving the FCC's mapping strategy, and how this can be
2364 achieved in a way that improves specifically broadband
2365 deployment in the underserved rural areas?

2366 *Mr. Von Ah. Thank you for that question,
2367 Representative Joyce.

2368 Our recommendations have been around getting Federal

2369 agencies to be more uniform in their reporting of their
2370 deployment data to the maps so that we understand where there
2371 are Federal obligations for a build-out and where there still
2372 is service lacking. So we have those open recommendations.
2373 We are working with the agencies to close them and to get
2374 sort of agreement amongst them all, but that is what our
2375 recommendations are.

2376 *Mr. Joyce. Led by Congresswoman Houchin, who just
2377 spoke to you, H.R. 4950, the Data BRIDGE Act, seeks to
2378 improve the FCC's existing National Broadband Map to include
2379 a layer specifically for agricultural areas. Representing
2380 rural Pennsylvania, I am grateful to Congresswoman Houchin
2381 for leading this legislative effort, and I am proud to join
2382 in and cosponsor that legislation.

2383 Mr. Von Ah, in your opinion, how would this mapping
2384 addition create the opportunity for more Federal grant
2385 dollars to reach these areas that the coverage is needed in
2386 so desperately?

2387 *Mr. Von Ah. I think our work has shown, again, more
2388 specific and more accurate data in the maps will help spur
2389 investment into those areas that are of greatest need.

2390 *Mr. Joyce. Do you have -- Mr. Von Ah, do you have any
2391 other suggestions for this subcommittee as we continue to
2392 work towards closing that digital divide completely?

2393 *Mr. Von Ah. Well, I think what is important going

2394 forward is once these programs that are all actively
2395 deploying broadband infrastructure sort of get to an end
2396 point, how are those networks going to be sustained over time
2397 and maintained over time? And I think that is sort of the
2398 question going forward for what a national broadband strategy
2399 would look like in the future.

2400 *Mr. Joyce. And those next steps need to be addressed
2401 right now, so thank you for bringing that into the
2402 discussion.

2403 We recognize that critical resources for rural
2404 communities such as precision agriculture, telemedicine, and
2405 even the ability to call 911 require dependable and reliable
2406 connectivity. Hard-working families in rural America built
2407 this nation. Their way of life must be preserved and
2408 supported by the modern technology that is available to so
2409 many Americans. And as we continue to seek ways to provide
2410 this infrastructure to every corner of our great country, I
2411 am proud to support Congresswoman Houchin's Data BRIDGE Act.
2412 It makes a strong step forward on the path to finally
2413 bridging the digital divide and ensuring that universal
2414 broadband availability reaches each and every corner of
2415 America.

2416 Thank you, Mr. Chairman, for allowing me to participate
2417 in this, and I yield back the remainder of my time.

2418 *Mr. Allen. The gentleman yields. I believe we have

2419 one more member on the way. We just got a notification.

2420 He is on his way in? Okay, bear with us a moment.

2421 [Pause.]

2422 *Mr. Allen. Okay, all right. Well, I am sorry, Mr.
2423 Obernolte is not going to be able -- he helps me a lot with
2424 all these kinds of things. He is really good with this.

2425 But seeing there are no further members wishing to be
2426 recognized, I would like to thank our witnesses for being
2427 here today. You pointed out a lot of things we have got to
2428 get done, we have got to get to work on, and I thank you for
2429 sharing that with us and then helping us to deal with these
2430 many issues that we have with technology and communications
2431 and everything else.

2432 I ask unanimous consent to insert in the record the
2433 documents included on the staff hearing documents list.

2434 Without objection, so ordered.

2435 [The information follows:]

2436

2437 *****COMMITTEE INSERT*****

2438

2439 *Mr. Allen. I remind members they have 10 business days
2440 to submit questions for the record, and I ask the witnesses
2441 to respond to those questions promptly. Members should
2442 submit their questions by the close of business on August 5,
2443 2026.

2444 And without objection, the subcommittee is adjourned.

2445 [Whereupon, at 3:38 p.m., the subcommittee was
2446 adjourned.]