S. HRG. 114–671

CYBERSECURITY, ENCRYPTION AND UNITED STATES NATIONAL SECURITY MATTERS

HEARING

BEFORE THE

COMMITTEE ON ARMED SERVICES UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 14; SEPTEMBER 13, 2016

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.fdsys.gov/

U.S. GOVERNMENT PUBLISHING OFFICE

26–536 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma
JEFF SESSIONS, Alabama
ROGER F. WICKER, Mississippi
KELLY AYOTTE, New Hampshire
DEB FISCHER, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
JONI ERNST, Iowa
THOM TILLIS, North Carolina
DAN SULLIVAN, Alaska
MIKE LEE, Utah
LINDSEY GRAHAM, South Carolina
TED CRUZ, Texas

JACK REED, Rhode Island
BILL NELSON, Florida
CLAIRE MCCASKILL, Missouri
JOE MANCHIN III, West Virginia
JEANNE SHAHEEN, New Hampshire
KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
JOE DONNELLY, Indiana
MAZIE K. HIRONO, Hawaii
TIM KAINE, Virginia
ANGUS S. KING, JR., Maine
MARTIN HEINRICH, New Mexico

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

CONTENTS

JULY 14, 2016

SEPTEMBER 13, 2016

CYBERSECURITY AND UNITED STATES NATIONAL SECURITY

THURSDAY, JULY 14, 2016

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:33 a.m. in Room SD–G50, Dirksen Senate Office Building, Senator John McCain (chairman) presiding.

Committee members present: Senators McCain, Ayotte, Fischer, Cotton, Ernst, Sullivan, Reed, Nelson, McCaskill, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, and King.

OPENING STATEMENT OF SENATOR JOHN McCAIN

Chairman MCCAIN. Good morning to all of our witnesses. We are pleased to have with us a distinguished panel of expert witnesses who each bring a unique perspective to this important issue of cybersecurity, encryption, and U.S. national security: Cyrus Vance, Jr., who currently serves as Manhattan district attorney; Chris Inglis, former deputy director of the National Security Agency and a professor cybersecurity studies at the U.S. Naval Academy; and Kenneth Wainstein, a former Homeland security adviser and assistant attorney general for national security at the Department of Justice during the Bush administration and now partner at Cadwalader.

I am sure it is a great organization.

[Laughter.]

Chairman MCCAIN. I thank each of our witnesses for appearing before the committee today.

I must note for the record that these were not our only invited guests. This committee extended an invitation to Apple CEO [Chief Executive Officer] Tim Cook to offer his perspective on these important issues. He declined.

I hope he will reconsider in the future so that this committee can benefit from the widest possible variety of perspectives.

End-to-end encryption allows communications and data shared across devices and platforms to be seen only by the individuals holding the device. The information on the device cannot be accessed in most cases by the company and in nearly all cases by the government, even with a lawful court order backed by probable cause.

Major American technology companies have made this level of encryption the default setting on their devices, meaning that even the least sophisticated lone wolves can operate in digital secrecy.

Terrorist groups like ISIL [The Islamic State of Iraq and the Levant] have taken notice. ISIL's backward ideology and brutal tactics may be a throwback to medieval times, but these terrorists are also effectively using modern technological tools. Indeed, encryption is now ubiquitous across the counterterrorism fight, providing an avenue for recruitment and radicalization, as well as the planning and coordination of attacks that pose an increasingly difficult challenge to intelligence collection, military operations, and law enforcement.

Put simply, encryption is eroding the digital advantage our national security and intelligence officials once enjoyed. That is why the topic of encryption concerns the Senate Armed Services Committee.

We must also recognize that encryption is not just a national security issue concerning terrorists in distant lands. Encryption is being used to shield criminals that terrorize communities across the Nation every day.

As Mr. Vance will testify, there are thousands of lawfully seized iPhones and other devices in the hands of law enforcement today that are completely inaccessible because their manufacturers refuse to comply with court-issued search warrants. The result is that thousands of murder, child sex abuse, and human trafficking cases are not being fully investigated.

Let there be no doubt the job of our national security agencies and our local, State, and Federal law enforcement is getting harder and the threat is growing. However, this is a complex problem with no easy solutions.

Encryption technology protects our most common and essential day-to-day Internet activities and safeguards our Nation's secrets from sophisticated cyber adversaries. We must carefully balance our national security needs and the rights of our citizens.

While we must recognize that authoritarian regimes are eager to gain keys to encrypted software so they can further their own abusive policies, we must also resist slipping into a false moral equivalence. Not all governments are the same. Not all surveillance is the same. Complying with valid search warrants in countries that uphold the rule of law does not create an obligation for technology companies to assist repressive regimes that undermine the rule of law in suppressing dissent or violating basic human rights.

Yes, this is a difficult problem. Ignoring this issue is not an option, nor is meeting all efforts to reach a middle ground with absolute resistance, as too many technology companies have done.

An all-or-nothing approach to encryption that is making it difficult and sometimes impossible to prosecute murderers, pedophiles, human traffickers, and terrorists is simply unacceptable.

I believe there is a growing recognition that the threat posed by the status quo is unacceptable and that we need the public and private sectors to come together to eliminate cyber safe havens for terrorists and criminals.

The struggle between security and privacy, or between public and private goods, is not new. These struggles are as old as our republic. We have not always gotten it right, but when we found that

balance, it has always been through open and honest dialogue. That is what we need right now.

Beyond encryption, I remain concerned by the administration's failure to provide the Department of Defense, the National Security Agency, and others with the necessary policy guidance to effectively defend, deter, and respond to our adversaries in cyberspace.

To be sure, there has been important progress, including the willingness of the administration to carry out and more openly discuss offensive cyber operations against ISIL. Still, policy deficiencies from deterrence to rules of engagement to arbitrary limitations on geographic areas of operations, and cyber collateral damage, all must be addressed.

Rather than answering these hard policy questions, it seems the White House continues to micromanage every cyber issue on a case-by-case basis.

Finally, as the role of Cyber Command continues to mature, some have suggested that we should reevaluate the "dual-hack" relationship between Cyber Command and NSA [National Security Agency]. Whether in the context of possibly elevating Cyber Command to a unified command or in its current role, we must be careful not to prematurely sever this important relationship.

I welcome the views of our witnesses, especially Mr. Inglis, as to whether, at some point in the future, it may make sense for Cyber Command to stand independent of NSA.

Once again, I thank our witnesses for their appearance before the committee today. I look forward to their testimony.

Senator Reed?

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman, for having this second hearing on encryption. I, too, want to welcome our trio of very distinguished witnesses and thank them for their many years of service to the Nation.

Mr. Vance, your leadership on this issue is commendable and your statement eloquently articulates your position. I also want to note that District Attorney Vance is advocating for legislation on only one element of the overall encryption debate which he considers most critical for law enforcement, the ability to access data stored on the most modern versions of the leading smart phones in the custody of the courts or the police.

Mr. Wainstein had a distinguished career in the FBI [Federal Bureau of Investigation] before being appointed the first assistant attorney general for national security and then as Homeland security adviser to President Bush. He has seen this issue evolve over time.

Thank you, Mr. Wainstein.

Mr. Chris Inglis is a graduate of the Air Force Academy with decades of experience at NSA, including over 7 years as deputy director. He has taught at both West Point and the Naval Academy, to try to make up for his previous situation.

You now occupy the chair of cybersecurity at the Naval Academy.

Thank you, Mr. Inglis.

Cyber is an issue that touches many committees in Congress. To the extent that it advances commercial encryption technology, and

the ease with which effective commercial encryption is applied adversely impacts foreign intelligence collection and counterterrorism, this committee has a strong and vital role to play and needs to be informed.

Law enforcement, in contrast, is not directly in our jurisdiction. As the FBI's dispute with Apple in the San Bernardino terrorist case shows, the inability of law enforcement agents to physically unlock smart phones and retrieve unencrypted data can directly impact national security.

I look forward to further exploring these types of issues with our witnesses.

I also want to note that there are other distinguished national security experts who provide competing advice on this complex issue. National experts such as Admiral Mike McConnell, former Director of National Intelligence, director of NSA; General Mike Hayden, former deputy director of NSA and CIA [Central Intelligence Agency]; and former Deputy Secretary of Defense Bill Lynn; and also former Secretary of Homeland Security Michael Chertoff, all oppose government mandates on commercial industry to enable access to unencrypted content.

This is an issue I would love to discuss with the panel when we get to your questioning.

They argue that cyber vulnerabilities are the greater threats to the public and national security, that previous predictions of disastrous consequence from commercial encryption technology failed to materialize, that U.S. Government access mandates will harm U.S. companies and provide cover for repressive regimes to suppress dissent, and that previous attempts to control encryption technologies for legislation did not succeed.

These experts have written an article explaining their views. Mr. Chairman, I would like to these articles part of the record.

Chairman MCCAIN. Without objection.

[The information referred to follows:]

The Washington Post

Opinions

Why the fear over ubiquitous data encryption is overblown

Clarification: *Due to a production error, a version of this column was temporarily posted prematurely before the editing process was complete.*

By Mike McConnell, Michael Chertoff and William Lynn July 28, 2015

Mike McConnell is a former director of the National Security Agency and director of national intelligence. Michael Chertoff is a former homeland security secretary and is executive chairman of the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. William Lynn is a former deputy defense secretary and is chief executive of Finmeccanica North America and DRS Technologies.

More than three years ago, as former national security officials, we penned an op-ed to raise awareness among the public, the business community and Congress of the serious threat to the nation's well-being posed by the massive theft of intellectual property, technology and business information by the Chinese government through cyberexploitation. Today, we write again to raise the level of thinking and debate about ubiquitous encryption to protect information from exploitation.

In the wake of global controversy over government surveillance, a number of U.S. technology companies have developed and are offering their users what we call ubiquitous encryption — that is, end-to-end encryption of data with only the sender and intended recipient possessing decryption keys. With this technology, the plain text of messages is inaccessible to the companies offering the products or services as well as to the government, even with lawfully authorized access for public safety or law enforcement purposes.

The FBI director and the Justice Department have raised serious and legitimate concerns that ubiquitous encryption without a second decryption key in the hands of a third party would allow criminals to keep their communications secret, even when law enforcement officials have court-approved authorization to access those communications. There also are concerns about such encryption providing secure communications to national security intelligence targets such as terrorist organizations and nations operating counter to U.S. national security interests.

Several other nations are pursuing access to encrypted communications. In Britain, Parliament is considering requiring technology companies to build decryption capabilities for authorized government access into products and services offered in

that country. The Chinese have proposed similar approaches to ensure that the government can monitor the content and activities of their citizens. Pakistan has recently blocked BlackBerry services, which provide ubiquitous encryption by default.

We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.

First, such an encryption system would protect individual privacy and business information from exploitation at a much higher level than exists today. As a recent MIT paper explains, requiring duplicate keys introduces vulnerabilities in encryption that raise the risk of compromise and theft by bad actors. If third-party key holders have less than perfect security, they may be hacked and the duplicate key exposed. This is no theoretical possibility, as evidenced by major cyberintrusions into supposedly secure government databases and the successful compromise of security tokens held by a major information security firm. Furthermore, requiring a duplicate key rules out security techniques, such as one-time-only private keys.

Second, a requirement that U.S. technology providers create a duplicate key will not prevent malicious actors from finding other technology providers who will furnish ubiquitous encryption. The smart bad guys will find ways and technologies to avoid access, and we can be sure that the "dark Web" marketplace will offer myriad such capabilities. This could lead to a perverse outcome in which law-abiding organizations and individuals lack protected communications but malicious actors have them.

Finally, and most significantly, if the United States can demand that companies make available a duplicate key, other nations such as China will insist on the same. There will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications to a wide spectrum of governmental access regimes with varying degrees of due process.

Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interests. After all, political power and military power are derived from economic strength. If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential. And that imperative may outweigh the tactical benefit of making encrypted communications more easily accessible to Western authorities.

History teaches that the fear that ubiquitous encryption will cause our security to go dark is overblown. There was a great debate about encryption in the early '90s. When the mathematics of "public key" encryption were discovered as a way to provide encryption protection broadly and cheaply to all users, some national security officials were convinced that if the technology were not restricted, law enforcement and intelligence organizations would go dark or deaf.

As a result, the idea of "escrowed key," known as Clipper Chip, was introduced. The concept was that unbreakable encryption would be provided to individuals and businesses, but the keys could be obtained from escrow by the government under court authorization for legitimate law enforcement or intelligence purposes.

The Clinton administration and Congress rejected the Clipper Chip based on the reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the '90s and into the new century.

Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.

Read more on this issue:

The Post's View: Putting the digital keys to unlock data out of authorities' reach

The Post's View: Compromise needed on smartphone encryption

Cyrus R. Vance Jr.: Apple, Google threaten public safety with default smartphone encryption

Gen. Michael Hayden Gives an Update on the Cyberwar

Former head of the CIA and NSA says government moves to protect cyberspace are too little, too late

Feb. 9, 2016 10:49 p.m. ET

We're in a global cyberwar in which our corporate secrets are our chief prize. Are we up for the fight?

To get a clearer answer, The Wall Street Journal's John Bussey spoke with Gen. Michael Hayden, principal of Chertoff Group and former director of the Central Intelligence Agency and National Security Agency. Here are edited excerpts of the discussion.

It's up to you

MR. BUSSEY: *We got some news last month. There's some legislation meant to increase cooperation between the government and business. Tell us about the bill and whether or not it helps CIOs protect corporate secrets.*

JOURNAL REPORT

- Read more at WSJ.com/LeadershipReport

MORE IN CIO NETWORK

- Hilary Mason, Andreas Weigend on the Mistakes Companies Make With Big Data
- Dawn Lepore Discusses the Path from CIO to CEO
- Andy Ozment on the Cybersecurity Information Sharing Act
- Jeremy Bailenson Peers Into the Future of Virtual Reality
- Andy Bryant Says CIOs Need Better Communications Skills

GEN. HAYDEN: We're talking about CISA, the Cybersecurity Information Sharing Act. Good news, a step in the right direction. But it's too long in coming, it's too small a step. And it reveals that within any realistic planning horizon, you are largely responsible for your own defense in the cyber domain.

The government, our government will be permanently late for your cybersecurity. Look, your armed forces view cyber as a domain. Land, sea, air, space, cyber. It's a new domain. You and I have decided that this domain is so wonderful, empowering, we're going to take things we used to keep down here in a safe, in a drawer, in a wallet, and put it up here where it's largely undefended. This is the largest ungoverned space in recorded human history. There is no rule of law up here.

As taxpayers, you and I are going to want our government to defend us up here the way we have become accustomed to relying on the government for defending us down here. But there's the general sclerosis of government, and the technology is going to move much faster than any government can move. Then we have not yet decided what it is we want or what it is we will allow the government to keep us safe. You're going to have to be responsible for your safety [in the cyber domain] in a way in which you have not been required to be responsible for your safety [in the physical domain] since the closing of the American frontier in 1890.

Who follows whom?

MR. BUSSEY: *It does seem that before the war on cybersecurity can be fought as a nation, we have to resolve the civil war internally over privacy.*

GEN. HAYDEN: Yeah. And that's a multigenerational thing. We haven't arrived at a national consensus. In the American system, when the government doesn't show up, we generally pick up the burden ourselves. So, the good news is there's a lot of private-sector activity designed to keep us safe.

Let me explain this another way. When I think about a national-security problem, generally my instincts are the government is the prime mover. If you're into Civil War history, Gen. Grant or Gen. Lee says, "You, sir, your corps is the main body. And you, gentlemen, you will conform your movements to the movements of the main body." In government, I assumed that in cyberdefense, the main body was the government, and you shall conform your movements with the movements of the main body. In the cyber domain, you are the main body. What our government has to teach itself is that the government needs, in all but a few exceptional cases, to conform its movements to the movements of the main body, you.

MR. BUSSEY: *One of the things that the private sector is doing is to look again at encryption.*

GEN. HAYDEN: The issue here is end-to-end unbreakable encryption, should American firms be allowed to create such a thing. You've got Jim Comey, the director of the FBI, saying, "I am really going to suffer if I can't read Tony Soprano's email or if I've got to ask Tony for the PIN number before I get to read Tony's emails." I get it. There is an unarguable downside to unbreakable encryption. On the other side is the question: On balance, is America more or less secure with unbreakable end-to-end encryption, regardless of whether Jim can read Tony's emails?

I think Jim Comey's wrong. Jim's logic is based on the belief that he remains the main body and you should accommodate your movements to the movements of him, which is the main body. And I'm telling you, with regard to the cyber domain, he's not. You are.

MR. BUSSEY: *Tell us how the landscape of threat is evolving or changing.*

GEN. HAYDEN: The stealing-your-data stuff is there, and it's getting worse. Beyond that, [people are trying] not just to steal data, but to create effects. So you've got Stuxnet, which is the destruction of a thousand centrifuges at Natanz in Iran. I view it as an unalloyed good, but it was done using a weapon comprised of ones and zeros to create physical destruction.

Leon Panetta spent a lot of time in his last year or two in government talking about cyber Pearl Harbor, digital 9/11, catastrophic attack. I don't think that's what we have to worry about. I'm not frightened about the Chinese turning out all the lights east of the Mississippi. I'm not worried about that superpower, catastrophic attack.

I'm worried about the isolated, nothing to lose, "Ah, what the hell? Let's go see what happens," nation state who goes after a North American enterprise to create physical destruction to show that they can. The Sony attack is the poster child for that.

Senator REED. Thank you very much, Mr. Chairman.

I believe one of the most important functions of our hearing is to illuminate and explain complex issues, and I hope our hearing today will make such a contribution.

Indeed, the series of hearings that the chairman has set up is absolutely critical, I think, to our consideration going forward, so I thank him for that.

Thank you, gentlemen. I look forward to your testimony.

Chairman MCCAIN. I thank the witnesses.

Mr. Vance?

STATEMENT OF CYRUS R. VANCE, JR., MANHATTAN DISTRICT ATTORNEY

Mr. VANCE. Thank you. Good morning, Chairman McCain,

Ranking Member Reed, and members of the Senate Committee on Armed Services.

On behalf of our office in New York City, on behalf of State and local law enforcement around the country, I am very grateful that you are willing to hear our testimony this morning.

The basic facts, Senators, underlying this debate, in my view, are really not that much in dispute.

First, just talking about Tim Cook's own statements that he made to the public and his customers in February of this year, it is absolutely true, as he said, that smart phones led by the iPhone have become an essential part of our lives. They certainly are an essential part of my life. As a citizen, I certainly appreciate the many benefits of the technological age and the Internet.

These devices are also essential to criminals. Our office investigates and prosecutes a range of cases from homicide to sex crimes, from international financial crime to crimes of terrorism. In all those crimes, and others, it is undisputed that criminals use smart phones to share digital information, to plan and commit crimes, whether through iMessages, photos, or videos.

Third, criminals know iPhones now enable them to communicate with impunity about those crimes. Let me tell you that the criminals are thrilled with this development.

Now, that is not hyperbole. In a real example from a case in my office, an incarcerated defendant on a pending sex crimes charge tells a friend that we overhear on a lawfully recorded landline out of Rikers Island jail, and I am quoting from the call, "Apple and Google came out with software that can no longer be unencrypted by the police. If our phones are running on iOS 8 software, they cannot open my phone. This may be another gift from God."

Senators, it is clear this is not a gift from God. It is a gift, perhaps unintended, from the two largest technology companies in the world.

Fourth, Apple's and Google's decision to limit law enforcement access, even with a court warrant, to critical information is, I believe, made under a questionable claim of increased privacy.

The encryption Apple provided on its mobile devices before iOS 8, that is, before the end of September 2014, was both secure for its customers and amenable to court- authorized searches.

Apple itself characterized the iOS 7 operating system as the ultimate in privacy, touting its proven encryption methods and ensur-

ing users that iOS 7 could be used with confidence in any personal or corporate environment.

Now, given Apple's own statements about iOS 7, shortly after Apple's reengineering of its phones to prevent search warrant access by law enforcement, I asked Apple in a letter dated March 2015 whether there was a bona fide security reason to make its new operating system, iOS 8, warrant- proof. Now, Apple chose not to answer me.

In March of this year, the House Judiciary Committee compelled Apple to answer the same question. That committee asked Apple the following question *in writing,* and I am quoting from the committee, "Was the technology you possess to decrypt these phones," the reference is to iOS 7 and their predecessors, "ever compromised?" That was the question to Apple.

Apple's written response was, and I am quoting the response, "The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems was not, to our knowledge, compromised."

Now Apple's answer to this crucial question shows what we have long suspected, that Apple's method of data extraction under iOS 7 posed no documented security problems.

That being so, I believe there should be no unreasonable security risk in a going-forward solution, if court-ordered warrants can be honored by extracting responsive data off the smart phones.

Now we know, I believe now, the risk of loss of security, on the one hand, may have been exaggerated. I know, on the other hand, speaking on behalf of law enforcement, that I can document the impact of warrant-proof devices on the security of the residents in my community.

Let me give you, if I may, an impact of this new encryption protocol introduced by Apple.

In my office alone, we now have more than 310 lawfully seized iPhones running iOS 8 or 9 that are completely inaccessible, despite court-ordered search warrants having been issued for them. These devices represent hundreds of real crimes against New Yorkers that we cannot fully investigate, including cases of homicide, child abuse, human trafficking, assault, cybercrime, and identity theft.

Now, that is just my office. The data from across the country tell a similar story.

In California, the Los Angeles County Sherriff's Department has amassed more than 150 inaccessible devices. The L.A. Police Department has more than 300. The Roseville Police Department has more than 200. Riverside County, California, has 12 inaccessible devices connected just to murder cases alone. The Charlotte-Mecklenburg Police Department in North Carolina has 160 inaccessible devices. In Texas, the Harris County DAs office collected more than 100 inaccessible devices in 2015 and have encountered 8 to 10 inaccessible devices per month so far this year. In Massachusetts, the Suffolk County DA representing Boston has 129 inaccessible devices.

Now this brief list shows the problem from the perspective of some members of State and local law enforcement.

Even this small sampling represents more than 1,000 cases in which local prosecutors lacked the evidence that we need, and that juries demand, to hold criminals accountable, in some cases exonerate the innocent, and deliver justice for victims and safety in our streets.

Now it is, respectfully, in my view, no answer to suggest, as some have, that government should develop the capacity to hack into these devices. In my opinion, a technological arms race between the Federal Government and Silicon Valley is not in our collective interest.

The enormous cost and energy of such a conflict are better directed, in my opinion, against our common enemies, the criminals.

Furthermore, local law enforcement agencies do not have the resources to access each lawfully seized device and would be required to send each device to costly third-party companies for analysis and data extraction.

According to the reports, the FBI paid in the neighborhood of $1 million to bypass the terrorist passcode in the San Bernardino case. I can assure you that amount represents more than the budgets for all law enforcement in many counties across the country.

Despite the large number of experts in the field of digital forensics and cryptology, such experts are still several models behind Apple's iPhones. The method employed to open Syed Farook's iPhone in the San Bernardino case reportedly works only on that particular iPhone, and only until Apple finds and patches the flaw the FBI was able to exploit.

Senators, surely the solution to the encryption problem is not a technological arms race. It is, in my opinion, Federal legislation.

I appreciate that some are skeptical of Federal regulation. Federal regulation of consumer products that impact public safety has been a part of our legal landscape for more than 100 years. Numerous industries, especially in financial services, are required by Federal regulators to retain data expressly for the purpose of helping to combat fraud and other wrongdoing.

Federal regulation is already important in the communications industry. When telephone companies went from using copper wires to using fiber optics and digital signals, the police could no longer use their old techniques of executing wiretap orders, so Congress passed CALEA [Communications Assistance for Law Enforcement Act], mandating that telecom providers build into their systems mechanisms for law enforcement to install court-ordered wiretaps.

Many of these regulations initially faced resistance, and the affected industries argued that the regulations were imposing upon individuals' privacy interests. Over time, the regulations have been accepted. It is clear that they play an important part in our society, especially in keeping people safe from harm.

Now our office's proposed solution, which was proposed in a white paper that we published in September 2014, is to enact a Federal statute providing that data on any smart phone made or sold in the United States needs to be accessible, not by law enforcement, but by the designer of the phone's operating system when the company is served with a valid search warrant issued by a court.

If a person or entity such as Apple offers encryption software, it has to have the ability to provide data, also in response to judicial order.

The solution, as I say is spelled out in our 2015 report, does not require new technology or any government backdoor. Under this solution, Apple would be able to comply with judicial warrants and offer the same strong encryption that it employed without, to our knowledge, a single documented breach before it adopted the default device encryption under iOS 8.

The focus of the proposed legislation, we believe, is appropriate because, since September 2014, our primary obstacle in local law enforcement has involved getting access to data at rest on the smart phones in our possession. That would be no small achievement, because it is local law enforcement that prosecutes more than 95 percent of the criminal cases in this country.

As it stands today, Apple and Google, not a court, not Congress, decide who has access to key evidence in criminal investigations and trials. I cannot and I do not believe it is right that two private companies should decide which victims can achieve justice in our country.

There has been discussion about convening task forces to examine the science and policy implications of default device encryption. That may well be a good step, but I urge Congress to act quickly. Twelve months of taking testimony resulting in nonbinding recommendations in a report will not adequately address the urgency of the problem that local law enforcement faces.

Time is simply not a luxury that local law enforcement, crime victims, or communities can afford. Our laws require speedy trials. Victims are waiting for justice. Criminals must be held accountable before they can reoffend.

Centuries of jurisprudence hold that no item—not a home, not a file cabinet, and not a smart phone—is beyond the reach of a court order. Our access to data today is grounded in and limited by the Fourth Amendment, which authorizes only reasonable searches based on probable cause, supported by a particularized search warrant, issued by a neutral judge.

Senators, that burden, not warrant-proof encryption, I believe, is the strongest safeguard we have in balancing privacy and public safety.

Thank you very much.

[The prepared statement of Mr. Vance follows:]

PREPARED STATEMENT BY NEW YORK COUNTY DISTRICT ATTORNEY CYRUS R. VANCE, JR.

Good morning Chairman McCain, Ranking Member Reed, and members of the Senate Committee on Armed Services. On behalf of my office and our partners in state and local law enforcement, I thank the Committee for its work and attention to what is not only a critically important issue of national security, but also an issue of public safety and justice for crime victims in thousands of local jurisdictions across the United States.

The decision by Apple and Google to engineer their mobile devices to be, in effect, "warrant-proof" has upended the balance that we have long enjoyed between privacy and public safety. Without federal legislation to restore that balance, we have delegated to businesses like Apple and Google the power to set it themselves.

The debate over encryption and public safety has matured significantly since 2014. The issue has crossed over into mainstream consciousness, owing in large part

to Apple's public refusal to assist the FBI with unlocking a terrorist's iPhone in San Bernardino. The San Bernardino episode introduced many Americans for the first time to the problem posed by smartphone encryption in criminal investigations, and my office and our partners have gone to some lengths to demonstrate to the public and to policymakers the full scope of the challenge in each of our jurisdictions.

The basic facts underlying this debate are really not in dispute. First, as Tim Cook said himself in his open letter to customers dated February 16, 2016: "Smartphones, led by iPhone, have become an essential part of our lives."[1] As a citizen, I certainly appreciate the many benefits of the internet age.

Second, these devices are also essential to criminals. Our office investigates and prosecutes a wide range of cases—from homicide to sex crimes, from international financial crime to terrorism. In all those crimes and others, it is undisputed that criminals use smartphones to share digital information, and to plan and commit crimes, whether through iMessages, photos, or videos.

Third, criminals know iPhones now enable them to communicate with impunity about their crimes. The criminals are thrilled with this development. That is not hyperbole. In a real example from a case in my office, an incarcerated defendant on a pending sex crimes charge tells his friend on a lawfully recorded landline phone from jail, "Apple and Google came out with these softwares [sic] that I can no longer be [un]encrypted by the police . . . [i]f our phone[s are] running on iOS8 software, they can't open my phone. This may be [a]nother gift from God."

That is not a gift from God, but an unintended gift from two of the largest technology companies in the world.

Fourth, Apple and Google's decisions limit our access to critical information under a questionable claim of an increase in privacy. The encryption Apple provided on its mobile devices pre-iOS 8—that is, up until the end of September, 2014—was both secure for its customers and amenable to court-authorized searches. We have good cause to believe that because Apple itself characterized its iOS 7 operating system as the ultimate in privacy, touting its proven encryption methods, and assuring users that iOS 7 could be used with confidence in any personal or corporate environment.1A[2] Under iOS 7, Apple also maintained the ability to help—in Apple's own words—"police investigating robberies and other crimes, searching for missing children, trying to locate a patient with Alzheimer's disease, or hoping to prevent a suicide."1A[3] Which is to say, Apple itself had already demonstrated that strong encryption and compliance with court orders were not incompatible.

Given Apple's own statements about the security of iOS 7, shortly after Apple's re-engineering of its phones to prevent search warrant access by law enforcement, I asked it in a letter dated March 2015, whether there was a bona fide security reason to make its new operating system, iOS 8, warrant-proof.[4] Apple chose not to answer me, but in March of this year, the House Judiciary Committee compelled Apple to answer the same question. That Committee asked Apple the following question, *in writing,* "Was the technology you possessed to decrypt these phones"—and the clear reference is iOS7 phones and their predecessors—"ever compromised?" Apple's written response was: "The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems *was not, to our knowledge, compromised."*[5] (Emphasis added.)

Apple's answer to this crucial question shows what we have long suspected: That Apple's method of data extraction under iOS 7 posed no documented security problems. That being so, then there should be no unreasonable security risk going forward if we return to the procedure where court-ordered warrants can be honored by extracting responsive data off of smartphones.

Let me give you the impact of this new encryption protocol introduced by Apple. In my office alone, we now have more than 310 lawfully-seized iPhones running iOS 8 or 9 that are completely inaccessible, despite court-ordered search warrants hav-

---

[1] Tim Cook, "A Message to Our Customers" (Feb. 16, 2016), *http://www.apple.com/customer-letter/*.

[2] See Apple, "iOS Security" (May 2012), at p. 2,

[3] Apple, "Apple's Commitment to Customer Privacy" (June 16, 2013), *http://www.apple.com/apples-commitment-to-customer-privacy/*.

[4] Letter from Cyrus R. Vance, Jr. to Jane Horvath, Senior Director of Global Privacy for Apple, Inc. (March 31, 2015), attached as Appendix II to the Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety (Nov. 2015), *http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.*

[5] Bruce Sewell, Senior Vice President and General Counsel for Apple, Inc., Responses to Questions for the Record, "The Encryption Tightrope: Balancing Americans' Security and Privacy," at p. 2. *http://docs.house.gov/meetings/JU/JU00/20160301/104573/HHRG-114-JU00-Wstate-SewellB-20160301-SD001.pdf.*

ing been issued for them. These devices represent hundreds of real crimes against New Yorkers that we cannot fully investigate, including cases of homicide, child sex abuse, human trafficking, assault, cybercrime, and identity theft.

The data from across the country tells a similar story. In California, the Los Angeles County Sheriff's Department has amassed more than 150 inaccessible devices, the Los Angeles Police Department has more than 300, and the Roseville Police Department has more than 200. Riverside County, California has 12 inaccessible devices connected to murder cases alone. The Charlotte-Mecklenburg Police Department in North Carolina has 160 inaccessible devices. In Texas, the Harris County District Attorney's Office collected more than 100 inaccessible devices in 2015 and have encountered 8 to 10 inaccessible devices per month so far this year. In Massachusetts, the Suffolk County District Attorney's Office has 129 inaccessible devices.

My brief list shows the problem from the perspective of some members of state and local law enforcement. Even this small sampling represents more than one thousand cases in which local prosecutors lack the evidence that we need—and that juries demand—to hold criminals accountable, exonerate the innocent, and deliver justice for victims and safety in our streets.

Some have argued that we now live in a "Golden Age of Surveillance," and therefore, prosecutors do not need smartphone evidence to effectively do our jobs. They frequently point to the availability of metadata, which is what we can obtain from a wireless carrier. Metadata typically consists of the time at which a call was placed or a message sent, and the phone numbers of the parties to that call or message. Metadata, while useful, is extremely limited because it does not include the substance of a call or message. With metadata, I can show that two people spoke before a criminal incident, but I cannot show what they said, and that information, of course, will be critical for proving their intent and the scope of their agreement.

The same is often true for social media—it can be a good tool for figuring out whether people know each other, but in many cases, it does not provide the level of content that we need to make our case. For law enforcement to investigate, prosecute, and exonerate most effectively, we need access to substantive evidence when we have a court order.

The problems created by default device encryption manifest themselves differently in almost every criminal case. Without critical evidence on smartphones, prosecutors may not be able to secure the most serious charge, but instead can only seek a lesser offense. As an example, my office recently handled a case where we had strong reason to believe that the defendant was running a human trafficking operation. With evidence from that defendant's smartphone locked behind a passcode known only to him, and existing solely on his device, we could only charge a far less serious offense, Promoting Prostitution, which carries less stringent penalties than human trafficking.

In other cases, there may be co-conspirators to the criminal scheme, but without the substance of their communication with defendants, prosecutors cannot charge those co-conspirators at all. In other cases still, the defendant may have victimized additional people, but prosecutors cannot charge the defendant for those additional crimes without evidence contained on smartphones.

In my view, it is no answer to say, as some suggest, that "government" should develop the capacity to hack into devices. A technological arms race between the Federal Government and Silicon Valley is not in our collective interest. The enormous cost and energy of such a conflict are better directed against our common enemies, criminals.

Furthermore, local law enforcement agencies do not have the resources to access each lawfully-seized device. Many lack in-house forensics labs, and would be required to send each device to costly, third-party companies for analysis and data extraction. According to reports, the FBI paid upwards of a million dollars to bypass the terrorist's passcode in the San Bernardino case. That amount represents more than the budgets for all law enforcement agencies in many counties around the country.

Despite the large number of experts in the field of digital forensics and cryptology, such experts are still several iPhone models behind Apple. The method employed to open Syed Farook's iPhone in the San Bernardino case reportedly works only on that particular model iPhone and that particular operating system, and only until Apple finds and patches the flaw that the FBI was able to exploit.

The solution to the encryption problem is not a technological arms race. It is federal legislation. I appreciate that some are skeptical of federal regulation, but federal regulation of consumer products that impact public safety has been a part of our legal landscape for over 100 years, and numerous industries, especially in financial services, are required by federal regulation to retain data expressly for the purpose of helping to combat fraud and other wrongdoing. Many of these regulations

initially faced resistance, and the affected industries argued that the regulations were imposing upon individuals' privacy interests. Over time, the regulations have been accepted, and it is clear that they play an important part in our society, especially in keeping people safe from criminal harm.

Federal regulation is already important in the communications industry. When telephone companies went from using copper wires to using fiber optics and digital signals, the police could no longer use their old techniques of executing wiretap orders, and so Congress passed the Communications Assistance for Law Enforcement Act (CALEA), mandating that telecom providers build into their systems mechanisms for law enforcement to install court-ordered wiretaps. CALEA has worked. It has saved lives, and it has withstood Constitutional challenge. It has not stifled innovation, as its opponents feared. It has not caused American consumers to migrate en masse to foreign competitors in search of greater privacy.

Also consider financial services, one of the most regulated industries in our country. As we learned more about how criminals were using banks to move money, Congress required firms to fight money laundering and to better know their customers—and specifically, to retain customers' data and make that data available to law enforcement with a court order. Over time, government and industry came together to work out compliance costs and procedures, and a broad consensus in favor of these rules emerged. The industry recognized that absolutism on customer privacy was not in its best interest. Banks and investment firms did not want to be conduits for crime and terror.

Here are a few other examples: DEA regulations require all U.S. pharmacies to maintain paper and electronic prescriptions bearing the name of the patient and prescriber, drugs dispensed, and dates filled. FTC regulations require any business that checks a customer's identification to maintain and provide victims and law enforcement with transaction records relating to identity theft. State regulations require private schools to maintain student data records, including records of attendance and suspected child abuse.

I could go on. The point is that companies in nearly every industry are required by law to maintain voluminous customer records and produce criminal evidence when they receive a court order. When your introduction of goods and services into the stream of commerce overlaps with public safety, this is the price of doing business in the United States. You cannot sell a car in this country unless it has dual air bags. Smartphone encryption, one of the great public safety challenges of our time, remains almost entirely self-regulated.

Apple and Google's position is that they must be exempt from these public safety obligations due to a cybersecurity risk unique to their sector. If we are going to make such an exemption—if we are going to agree to live with the collateral consequence of a little bit more crime and terror—then the need for this exemption must be grounded in sound data analysis. We need quantitative data—not rhetoric—to substantiate the benefits of unregulated, default device encryption on smartphones. If we are going to authorize—for the first time in our society—evidence-free zones, we need to be sure there was a problem that needed to be solved in the first place. We need to know what we are getting in exchange for trading away a measure of our public safety.

My office's proposed solution is to enact a federal statute providing that data on any smartphone made or sold in the United States must be accessible—not by law enforcement, but by the maker of the smartphone's operating system—when the company is served with a valid search warrant. If a person or entity such as Apple offers encryption software, it has to have the ability to provide data in response to a judicial order.

This solution—as spelled out in my office's *2015 Report on Smartphone Encryption and Public Safety*—requires no new technology, and no government backdoor. I want to make it clear that we do not want to ban encryption. There is probably no office in the country that deals with more cybercrime and identity theft cases than mine, so of course, we support strong encryption. Under our proposed solution, Apple would be able to comply with judicial warrants, and to offer the same strong encryption that it employed without a single documented breach before it adopted default device encryption in iOS 8.

This solution is limited to data at rest on smartphones. It would not affect encryption of data in motion. I cannot at this time offer a technical fix to address data in motion. I am confident, however, that engineers from industry and government, working together in good faith, can find one.

The focus of my office's proposed legislation is appropriate because since September 2014, our primary obstacle in local law enforcement has involved getting access to data at rest on smartphones that we possess. That would be no small

achievement because it is local law enforcement that prosecutes more than 95 percent of crimes committed in the United States.

As it stands today, Apple and Google—not a court, not Congress—decide who has access to key evidence in criminal investigations and trials. I cannot, and do not believe it is right, that two private companies should decide which victims can achieve justice.

There has been discussion about convening task forces to examine the science and policy implications of default device encryption. That may be a good step, but I urge Congress to act quickly. Twelve months of taking testimony resulting in non-binding recommendations in a report will not adequately address the urgency of the problem that local law enforcement faces. Time is not a luxury that local law enforcement, crime victims, or communities can afford. Our laws require speedy trials. Victims require justice. Criminals must be held accountable before they can reoffend.

Centuries of jurisprudence hold that no item—not a home, not a file cabinet, and not a smartphone—is beyond the reach of a judicial order. Our access to data is grounded in and limited by the Fourth Amendment, which authorizes only reasonable searches, based on probable cause, supported by a particularized search warrant, issued by a neutral judge. That burden, not warrant-proof encryption, is the strongest safeguard we have in balancing privacy and public safety.

Thank you for the opportunity to testify today.

Chairman MCCAIN. Thank you.

Mr. Inglis?

STATEMENT OF JOHN C. INGLIS, ROBERT AND MARY M. LOOKER, PROFESSOR IN CYBER SECURITY STUDIES, UNITED STATES NAVAL ACADEMY, AND FORMER DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. INGLIS. Thank you, Chairman McCain, Ranking Member Reed, and members of the committee. I am pleased to appear before you to talk today about cyber and encryption issues.

In my opening remarks, I would like to cover three areas.

First, I think it is important to lay out a framework of interests that can guide choices about desired or unwanted outcomes that transcend the technology discussions that so often dominate this debate.

Second, I would like to offer my view, in the context of encryption within the system of systems we once referred to as the telecommunications sector and now variously refer to as the Internet or cyberspace. There are, of course, surgical applications of encryption that can be considered in isolation, but these tend to be the exception rather than the rule, even if they are considerably more tractable.

Finally, I will suggest some implications of this discussion in the context of an increasingly interconnected world, one where it is unlikely that purely national solutions will either be acceptable or widely adopted.

First, framing the issues. In trying to simplify and untangle the various threads of this discussion, it is tempting to focus first and foremost on technology and, more particularly, encryption. One of the perils of that approach is that it fails to first establish a foundation of principles and objectives that can drive the attributes of technology and other systems intended to serve the interests of society.

There are, arguably, at least four interests converging here. The first is the desire by individuals for security of the communications and data that they transmit or store on digital devices and networks.

This interest is often oversimplified as a desire to protect confidentiality of data, sometimes shorthanded as protecting privacy. The services of integrity and availability are often just as important, delivering needed confidence to the integrity and resilience of financial transactions, personal preferences, and the flow of critical resources ranging from energy to airplanes, and the like. Encryption technology can and does make a contribution to all three.

The second interest in play here is the goal of protecting society from the actions of those who would use internet-based communications to plan, coordinate, and deliver harm to its collective security interests. This is not an idle threat and not a future prospect. These threats include, but are not limited to, the use of Internet-based communications to conduct illicit activities such as child pornography, terrorism, or the delivery of cyberthreats.

Indeed, it is the demonstrated potential for encryption to provide anonymity and cover to those who threaten our collective interests that underpins law enforcement and the intelligence community's desire to gain access to the content of individual communications.

The third interest in play is the desire of individuals or companies to freely innovate, create, share, and sell products in the marketplace without undue interference from government. The ability to do so, of course, is a vital component of U.S. freedoms and its economic and national security.

Building upon the third interest, a fourth interest emerges, namely the need for U.S. companies to remain competitive in what has become a global marketplace, a desire that is particularly acute for companies doing business across differing legal regimes where the balance struck between individual and collective security is uneven.

Solutions that arbitrarily deliver a unique advantage to one society above others will falter and fail in that world, risking not only a company's viability in foreign markets but the economic vitality and prosperity of the U.S. itself.

Taken individually, each of these aims can be viewed as a laudable goal. Taken in sum, an unqualified commitment to one of the aims necessarily makes it more challenging to achieve one or more of the others. Further, the dynamic nature of technology and its creative application to the myriad tasks by millions of users, hundreds of millions of users, greatly increases the difficulty of striking and sustaining a particular balance over time.

In any event, unless and until we determine which of these interests we want to support, we will be unable to judge the efficacy and suitability of any particular system, technology, or protocol.

My bottom line point would be the following. Some would argue that these four interests constitute a choice. I believe this is shortsighted. The U.S. Constitution, as already noted by the Senators leading the hearing, provides useful guidance here in the use of the word "and," not "or," as the conjunction joining the preamble's enumeration of goals motivating the formation of a more perfect union.

I am firmly convinced that the innovation, creativity, and industry exist to align and support all four of the interests I have outlined here.

Whatever the choice may be, the premise of our union is that we must establish the overarching goal before devising laws, procedures, and technologies that advance those stated interests.

There are two common misperceptions that often the cloud this debate vis-a-vis encryption. The first is that encryption stands on its own as a security tool. In practice, across the vast majority of security systems, encryption is just one of several mechanisms used in combination to deliver the desired mix of confidentiality, availability, and integrity. To be sure, it is an essential component of a globally deployed system protecting both data and motion and data at rest, but it is hardly sufficient in and of itself. Physical security, personnel security, user behaviors, hardware, software, security are all equally essential.

I do not point this out to detract from the necessary focus on the resilience of encryption schemes, but to say that we should not fool ourselves that a strong right arm on an otherwise undeveloped frame is enough to protect our interests. This will be ever true as technology continues to advance.

Second, and more important, is the misconception about encryption that it is a monolithic thing, that it is either on or that it is off. A quick look at the diversity of user expectations and vendor choices reveals that it is far more nuanced and complicated. Some users want their data encrypted so that they can be the only ones who can recover it—no vendor backups, no emergency recovery service, no possibility of third-party access or government surveillance.

Other users want a safety net, the ability to recover a lost key, retrieve lost data, backup data on some mediums, say the cloud, that is recoverable under a variety of circumstances.

Adding to that, vendor choices regarding their service offerings cater to this broad array of user preferences while adding an overlay of vendor-preferred attributes. Some vendors deliver encryption systems that cannot be penetrated by even the vendor himself or herself, either for their purposes or on behalf of others. Other vendors build and deliver systems that contain exceptional access mechanisms, built-in means to remove the overlay of encryption at various points in the transport or storage of that piece of data.

The commercial reasons for this exceptional access run the gamut from creating safety nets for users seeking to recover data to enabling access to data by a party other than the data owner—in some cases, the vendor himself or herself—because they want to actually access that content for purposes of their business proposition.

The result is an architectural landscape where some vendors place security controls wholly in the hands of users while others deliver systems that allow vendor or third parties to access user data because that access is essential to the vendor's business model.

The point is that these differing approaches are not generally portrayed as weak versus strong encryption. They are more properly differentiated by their choice of how and when the protected materials may be revealed.

This diversity of choices reflects, of course, the reality of a free market economy and the rights of individuals, including companies,

to pursue features of their own preference. As such, these choices are neither good nor bad. They are just choices.

This diversity suggests there is no one design principle driving the use of encryption. If we assume that these same market forces will deliver a principled reconciliation, if not an alignment, of societal goals that will endure over time, we should only look at the diverse user expectations, the diverse technologies in the marketplaces, and remember the excesses periodically delivered by markets to come to a different conclusion that that is not the solution.

In the face of this natural diversity and architectural choices, the use of terms like backdoors and secret keys must be seen as pejorative and unhelpful. It is ultimately determined by a system designer that it is appropriate to provide a means for exceptional access through some party other than the data owner.

Generally, they ask three questions. Is there a legitimate purpose being served? Does the data owner understand the nature if not the details of the potential access? Are the controls on the access sufficient to ensure that such access is constrained to the identified purpose?

In summarizing, I would like to actually tease out some implications enumerated or perhaps surfaced by those two broad topics of discussion.

First, the use of strong encryption is an essential component of security for our Nation and our citizens. The fundamental question is not whether to choose one purpose or another, but to determine how access to stored or transmitted data is controlled by the application of strong encryption that is technically feasible to do then.

Second, a framework to reconcile the various interests arguing for potentially different technical solutions will be best served by first reconciling if not aligning our societal goals.

Third, if our goal is to deliver security to individuals, and security for the American people writ large, and continued economic vitality in a global marketplace, then we must deliver these goals in a global context, neither surrendering nor wholly favoring U.S. security to the detriment of like-minded nations.

Along those lines, fourth, it is considerably more likely that law enforcement interests can be parsed into international norms than can national security interests. A bias, therefore, toward law enforcement interests in this area may be appropriate to deliver the framework that we seek and the attendant solutions that then work within that framework.

Fifth, as I have said before, market forces alone have seldom shown themselves able to deliver consistent alignment of societal outcomes across diverse products and services and typically have never done that across time.

Finally, inasmuch as I describe a mandate for government action in this space, I think government action is both required and must be fully informed by various interests government is formed to represent; focused on ensuring the various freedoms and rights of individuals while also maintaining collective security—we can do both; and mindful that the engine of innovation and delivery is almost exclusively found in the private sector.

To be clear, I do see a role for government in both facilitating the creation of an enduring values-based framework that will drive

technology and attendant procedures and in reconciling that framework to like-minded nations across the world.

Conversely, I believe government's failure to serve in this role will effectively defer leadership to a combination of market forces and the preference of other nation-states, which will drive unopposed solutions that we are likely to find far less acceptable.

In spirit, I applaud the initiative of this committee and the further work that it undertakes today, and I look forward to your questions.

[The prepared statement of Mr. Inglis follows:]

PREPARED STATEMENT BY CHRIS INGLIS

Thank you, Chairman McCain, Ranking Member Reed, and Members of the Committee. I am pleased to appear before you today to talk about cyber and encryption issues with a specific focus on the challenges to law enforcement caused by encryption.

The issues in play here are technically complex but, more importantly, cut across several distinguished interests that are not easily reconciled. Consistent with its powers under Article I, I believe the Congress will be an essential component of our ability to identify, create and sustain the framework needed to align the various interests in play.

My comments today are derived from twenty-eight years of experience at the National Security Agency working both of its related but distinguished missions: the Information Assurance mission supporting the defense of critical information and networks, and the Signals Intelligence mission which generates foreign intelligence needed to inform the Nation's defense. While I possess technical degrees in engineering and computer science, the majority of my career at the National Security Agency was spent in leadership positions, including seven and one half year's service as NSA's senior civilian and Deputy Director during the period 2006–2014.

In my opening remarks, I would like to cover three areas:

- First, I think it is important to lay out the framework of interests that can guide choices about desired, or unwanted outcomes that transcend the technology discussions that have so often dominated this debate.
- Second, I will offer my view on the context of encryption within the systems-of-systems we once referred to as the telecommunications sector and now variously refer to as the internet or cyberspace. There are, of course, surgical applications of encryption that can be considered in isolation but these tend to be the exception rather than the rule, even if they are considerably more tractable in sorting out desired outcomes and equities.
- Finally, I will suggest some implications of this discussion in the context of an increasingly interconnected world—one where it is unlikely that purely national solutions will either be acceptable or widely adopted.

FRAMING THE ISSUES IN PLAY:

In trying to simplify and untangle the various threads of this discussion, it is tempting to immediately focus on the technology, and more particularly encryption. One of the perils of that approach is that it fails to first establish a foundation of principles and objectives that can drive the attributes of technology and other systems intended to serve the interests of society.

There are arguably at least four interests converging here.

- The first is the desire by individuals for security of the communications and data they transmit across or store on digital devices and networks. This interest is often over-simplified as the desire to protect the *confidentiality* of data communicated across or stored in cyberspace—sometimes short-handed as "protecting privacy". The services of *integrity* and *availability* are often just as important—delivering needed confidence to the integrity and resilience of financial transactions, personal preferences, and the flow of critical resources ranging from energy to airplanes. Encryption technology can and does make a contribution to all three of the basic security services, transcending the issue of privacy alone.
- The second interest in play here is the goal of protecting society from the actions of those who would use internet based communications to plan, coordinate or deliver harm to its collective security interests. These threats include but are not limited to the use of internet based communications to conduct illicit activ-

ity such as child pornography, terrorism, or the delivery of cyber threats. Indeed, it is the demonstrated potential for encryption to provide anonymity and cover to those who threaten our collective interests that underpins law enforcement's and the intelligence community's desire to gain access to the contents of individual communications.

- The third interest in play here is the desire of individuals or companies to freely innovate, create, share and sell products in the marketplace without interference from government. Their ability to do so is, of course, a vital a component of U.S. freedoms and its economic and national security.
- Building upon the third interest, a fourth interest emerges, namely the need for U.S. companies to remain competitive in what has become a *global* marketplace, a desire that is particularly acute for companies doing business across differing legal regimes where the balance struck between privacy and collective security is uneven. Solutions that arbitrarily deliver unique advantage to one society above others will falter and fail in that world, risking not only a company's viability in foreign markets but the economic vitality and prosperity of the U.S. itself.

Taken individually, each of these aims can be viewed as a laudable goal. Taken in sum, an unqualified commitment to one of the aims necessarily makes it more challenging to achieve one or more of the others. Further, the dynamic nature of technology and its creative application to myriad tasks by millions of users greatly increases the difficulty of striking and sustaining a particular balance over time. Keeping up with this ever changing landscape has always been a challenge for the conduct of lawful surveillance by law enforcement or intelligence agencies. This is generally referred to by the law enforcement community as "going dark". Encryption is only one component of this challenge.

In any event, unless, and until, we determine which of these interests we want to support, we will be unable to judge the efficacy and suitability of any particular system, technology, or protocol.

Some would argue that these four interests constitute a choice. I believe this is shortsighted. The U.S. Constitution provides useful guidance here in its use of the word "and", not "or" as the conjunction joining the preamble's enumeration of goals motivating the formation of a "more perfect union": *"to provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves".*

I am firmly convinced that the innovation, creativity and industry exist to align and support all four of the interests I've outlined here. Whatever the choice may be, the premise of our union is that we must establish the overarching goal before devising laws, procedure and technologies that advance those stated interests.

ON THE NATURE OF "SECURE SYSTEMS"

There are two common misconceptions that often cloud this debate. The first is that encryption stands on its own as a security tool. In practice, across the vast majority of security systems, encryption is just one of several mechanisms used in combination to deliver the desired mix of confidentiality, availability and integrity. To be sure, encryption is an increasingly essential component of a globally deployed security system, protecting both data in motion and at rest, but it is hardly ever sufficient in and of itself. Physical security, personnel security, user behaviors, and hardware and software security are all equally essential components. This observation is not meant to detract from a necessary focus on the resilience of encryption schemes but we should not fool ourselves that a strong right arm on an otherwise underdeveloped frame is enough to protect our interests. This will be ever truer as technology continues to advance. By way of example, the possibility of quantum computing should remind us that our focus should be on determining principles that will endure across the inexorable roil of technology transformation.

The second, and more important, misconception about encryption is that it's a monolithic thing. That you either have it "on" or you don't.

A quick look at the diversity of user expectations and vendor choices reveals that it's far more nuanced and complicated.

Some users want their data encrypted so that only they can recover it. No vendor backups. No emergency recovery service. No possibility of third party access or government surveillance.

Other users want a safety net—the ability to recover a lost key, or retrieve lost data by backing it up on some medium, say the "cloud", that's recoverable under a variety of circumstances.

More significantly, vendor choices regarding their service offerings cater to this broad array of user preferences while adding an overlay of vendor preferred at-

tributes. Some vendors deliver encryption systems that cannot be penetrated by the vendor, either for its own purposes, or on behalf of others, whether that's the user or the government. Other vendors build and deliver systems that contain "exceptional access mechanisms"—built-in means to remove the overlay of encryption at various points in the transport or storage of a piece of data. The commercial reasons for this "exceptional access" run the gamut from creating safety nets for users seeking to recover data when they cannot remember or find their encryption keys, to enabling access to data by a party other than the data owner for the purpose of analyzing user content to tee up targeted advertising or other commercial offerings.

The result is an architectural landscape where some vendors place security controls wholly in the hands of the user while others deliver systems that allow the vendor, or third parties, to access user data because that access is essential to the vendor's business model. These differing approaches are not generally portrayed as weak versus strong encryption. They are more properly differentiated by their choice of how and when the protected materials may be revealed.

This diversity of choices reflects the reality of a free market economy and the rights of individuals, including companies, to pursue features of their own preference. As such, these choices are neither good nor bad. They're just choices. Moreover, this diversity in approach suggests that there is no one design principle driving the use of encryption, and most certainly there is no one way to make good use of it. If we assume that these same market forces will deliver a principled reconciliation, if not an alignment, of societal goals that will endure over time, diverse user expectations, and attendant technology transformation we need only observe the diversity of choices currently available, or remember the excesses periodically delivered by markets seeking private advantage for some company or segment of the private sector.

In the face of this natural diversity in architectural choices, the use of terms like "backdoors" and "secret keys" must be seen as pejorative and unhelpful. If it is ultimately determined by system designers that it is appropriate to provide a means for exceptional access for some party other than the data owner, the important questions will be: "Is there a legitimate purpose being served?" "Does the data owner understand the nature, if not the details, of the potential access?" and "Are the controls on the access sufficient to ensure such access is constrained to the identified purpose and not abused?"

Summarizing:

I will summarize my opening remarks by enumerating the key implications suggested by them:

First, the use of strong encryption is an essential component of security for our nation and our citizens. The fundamental question in such systems is how access to stored or transmitted data is controlled by the application of strong encryption.

Second, a framework to reconcile the various interests arguing for potentially different technical solutions in this debate will be best served by first reconciling, if not aligning, our societal goals before considering a particular implementation offered by one or more vendors, the government, or subject matter experts.

Third, if our goal is to deliver security for individuals, *and* security for the American people writ large, *and* continued economic vitality in a global marketplace for American industry then our framework must align and deliver these three goals in a global context, neither surrendering nor wholly favoring U.S. security to the detriment of like-minded Nations.

Fourth, it is considerably more likely that law enforcement interests can be parsed into international norms than can national security interests. A bias towards law enforcement's interests in this area may be appropriate to deliver a framework and attendant solutions that work across national boundaries and to address the more pressing needs of local law enforcement, which often lack the technical resources to pursue other means of accessing data pursuant to a lawful investigation.

Fifth, market forces, alone, have seldom shown themselves able to deliver a consistent alignment of societal outcomes across the diverse products and services of vendors at any time, and have never delivered one across time.

Finally, in as much as I describe a mandate for government action in this space, I think government action must be:

- Fully informed by the various interests government is formed to represent;
- Focused on ensuring the various freedoms and rights of individual citizens while also maintaining collective security;

and

- Mindful that the engine of innovation and delivery is almost exclusively found in the private sector.

To be clear, I do see a role for government both in facilitating the creation of an enduring, values based, framework that will drive technology and attendant proce-

dures to serve society's interests, and in reconciling that framework to-and-with like-minded Nations in the world.

Conversely, I believe government's failure to serve in this role will effectively defer leadership to a combination of market forces and the preferences of other nation-states which will drive, unopposed, solutions that we are likely to find far less acceptable.

In that spirit, I applaud the initiative and further work of this committee in taking up the matter and working through these difficult issues.

I look forward to your questions.

Chairman MCCAIN. Thank you.

Mr. Wainstein?

STATEMENT OF HONORABLE KENNETH L. WAINSTEIN, FORMER ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, DEPARTMENT OF JUSTICE

Mr. WAINSTEIN. Chairman McCain, Ranking Member Reed, members of the committee, thank you very much for the invitation to appear before you today.

As my colleagues have made clear, we are in the midst of a national debate over the implications of default encryption. This is a debate that has been going on for the better part of two years, and we now find ourselves at really what is a complete impasse. It is time, I urge, for Congress to step in and break through that impasse.

Congress has played a pivotal role over the years in striking a balance between individual and societal privacy interests on one hand, and our Government's law enforcement and national security interests on the other.

That is what it did when it passed title III and FISA, which mandated a judicial process for issuing warrants and orders for criminal and national security wiretaps. That is what it did when it passed the Communications Assistance for Law Enforcement Act, CALEA, that my colleague referenced, requiring telecommunications carriers to equip themselves to ensure the government can conduct lawfully authorized surveillance on their systems.

Despite these laws, gaps started to appear in our surveillance capabilities in the last decade, and government officials started to worry that they were going dark. This going dark issue has become exponentially more problematic with the recent advent of the default encryption, as a result of which providers and manufacturers are now often completely unable to satisfy lawful court surveillance orders.

This dilemma is now clear for all to see, and the lines of the debate have been drawn with government officials arguing that default encryption can endanger our country by creating safe places for criminals and terrorists to operate outside the reach of law enforcement and national security officials, and with representatives of the technology and civil liberties communities countering with a variety of arguments, including that any accommodation for government surveillance would undermine the security of encryption, that any accommodation would cause U.S. technology companies to lose customers who might be skeptical of a company that cooperates with the U.S. Government, and that any accommodation would simply cause wrongdoers to start using foreign encrypted

services as opposed to services here in the U.S. that are subject to that accommodation.

Citing these and other arguments, some of the technology and civil liberties communities have taken an absolutist position that there should be no government accommodation at all.

Now, while I fully appreciate the tremendous societal value of strong encryption, and I appreciate the validity of the technology industry's concerns, I do not believe that that is the end of the discussion. Our surveillance capabilities are just too important to our national security. It is due in large part to those capabilities that we have had success in protecting our country against large-scale terrorism since 9/11.

That record of success, however, is now being tested by the rise of ISIS, which clearly recognizes the operational value of encrypted communications, as it has issued its members guidance on encryption and it intentionally uses encrypted apps in its recruiting efforts.

With this gathering threat on the horizon, now is the time for Congress to mobilize and embark on a legislative process that calls on both sides of this debate to fully lay out the basis for their views.

For the government, this means completely explaining how significantly their different investigative efforts are or are not handicapped by the use of default encryption technologies. For the technology industry and civil liberties groups, this means providing hard data that demonstrates exactly how and how much each possible type of potential accommodation would impact their encryption system.

It is only when Congress receives this data that it can knowledgeably balance the potential cyber dangers posed by any government accommodation against the national security and law enforcement benefits of having one in place.

Congress can undertake this effort either through a traditional legislative process or through the establishment of a commission like that that has been proposed by Senator Warner and Chairman McCaul. Either of these options would be a significant step forward from where we are now.

The option that is not a step forward is the option of inaction and continued impasse. We have seen the consequences of that option before, as that was the option the government effectively pursued in the late 1990s and early 2000s when debating the wisdom of the wall, which was the regulatory barrier that prevented coordination and information-sharing between law enforcement and intelligence community personnel.

That inaction had tragic consequences when the existence of the wall contributed to our inability to identify the 9/11 hijackers and to prevent them from launching their attacks. Congress dismantled the wall when it passed the PATRIOT Act 6 weeks after 9/11, but that was too late for the 3,000 murdered Americans.

We made the mistake of inaction once before. We must not make it again.

I applaud the committee for holding today's hearing and showing leadership on this issue. It gives me hope that we can, in fact,

move beyond the current impasse and reach a workable solution to this critical problem.

My thanks again for inviting be here today, and I look forward to answering your questions.

[The prepared statement of Mr. Wainstein follows:]

PREPARED STATEMENT BY KENNETH L. WAINSTEIN

Chairman McCain, Ranking Member Reed, and distinguished Members of the Committee, thank you for the invitation to appear before you today. My name is Ken Wainstein. I am a partner at the law firm of Cadwalader, Wickersham & Taft, and I previously served as the Homeland Security Advisor to President George W. Bush, as the Assistant Attorney General for National Security, and in a variety of other positions in the Justice Department. Thank you for the opportunity to address the pressing national security issues raised by encryption.

I. INTRODUCTION

We are in the midst of a national debate that was triggered by the recent adoption of default encryption by large communications service providers. The debate is between those in government who insist there should be a technical accommodation allowing them to penetrate encryption and surveil criminal and terrorist communications and those in the technology and civil liberties communities who insist that any such accommodation would compromise encryption and jeopardize the security of our communications. This debate has been going on for about two years, and we now find ourselves at an impasse with neither side showing any sign of backing down.

It is time for Congress to step in and break through that impasse. Congress has long played a pivotal role in striking the balance between individual and societal privacy interests and our Government's law enforcement and national security interests. Congress should play that role once again by pushing both sides of this debate toward a solution to this impasse.

II. LEGAL BACKGROUND

Since the dawn of telephony, we have wrestled with the question of when and under what conditions government investigators should be allowed access to the content of private communications. In the 1967 decision Katz v. United States, the Supreme Court ruled that an individual has a reasonable expectation of privacy in the content of his or her phone calls, and the next year Congress passed title III of the Omnibus Crime Control and Safe Streets Act, mandating the process by which the government must make a probable-cause showing to secure a judicial warrant authorizing it to use a wiretap. After Congressional investigations in the 1970's revealed a series of surveillance abuses against persons like Dr. Martin Luther King, Jr., Congress passed the Foreign Intelligence Surveillance Act of 1978 ("FISA") creating a process of judicial review and approval for electronic surveillance to obtain information related to foreign intelligence, international terrorism, foreign espionage and other national security threats.

With the passage of title III and FISA, Congress struck a balance between the privacy interests in electronic communications and the legitimate needs of law enforcement and intelligence agencies to obtain access to those communications. While the balance Congress struck in each of these laws—and other laws addressing government investigative access to private information—may have been suitable at that time, that balance shifted with the evolution of technology in the ensuing years, which, in turn, triggered a series of national debates over how best to adapt existing laws to new technological realities. Over the past couple decades, Congress has done a very commendable job of brokering those debates and bringing the surveillance laws up to date. No better example was the legislative debate in 2007–08 that resulted in the FISA Amendments Act, a well-considered piece of legislation that realigned our foreign intelligence surveillance authorities to account for the revolution in communications technology since the passage of FISA in 1978.

Once each of those debates was resolved and the rules were legislatively established, government officials could then move forward to conduct the surveillance they needed. To get the judicial authorization, they provided the required predication and justification to the relevant court and received the court's authorizing warrant or order. Then, to get the warrant or order implemented, they served the relevant communications provider with a secondary order commanding the provider to execute the warrant or order.

III. GOING DARK

Over time, however, this process became less and less reliable as more and more providers were unable to give the government the assistance necessary to execute the authorized surveillances. With the exponential increase in the volume of electronic communications and the diversification of technologies from wire telephony to mobile voice communications over digital, switch-based services, many providers became either unable or unwilling to satisfy lawful wiretap requests. As a result, by the mid-1990's, law enforcement agencies saw that their surveillance capabilities were declining, and they started to worry that they were "going dark."

Congress responded to this concern in 1994 by passing the Communications Assistance for Law Enforcement Act ("CALEA"), which required telecommunications carriers to modify their equipment, facilities, and services to ensure that the government could conduct lawfully-authorized surveillances.

Despite CALEA, significant gaps remained in our surveillance capabilities. There were a number of companies that simply did not invest the money and time necessary to develop the capabilities to enable surveillance in their systems. In addition, there developed a broad range of communications technologies—like email, instant messaging, social networking sites and peer-to-peer services—that were simply not covered by CALEA. As a result, the government was increasingly unable to surveil its criminal and national security targets by the end of the last decade.

This "going dark" issue then became exponentially more problematic with the recent advent of default endpoint and end-to-end encryption. With endpoint encryption, the data is encrypted while stored on the communication device, and the encryption key is held by the device or the device owner, and not by the service provider or device manufacturer. Endpoint encryption became the default setting when Apple unveiled a new operating system for its iPhones and other devices in September 2014, and other service providers like Google have since followed suit. The problem was further compounded by the introduction of end-to-end encryption, in which the contents of a communication are encrypted in transit and neither the device manufacturer nor the telecommunications carrier possesses an encryption key. As a result of these default encryption processes, service providers and device manufacturers are now often unable to satisfy lawful court surveillance orders—a scenario that will increasingly put our law enforcement and national security officials in the dark as this technology becomes industry standard and our adversaries gravitate to it.

IV.GOING DARK GOING FORWARD

This dilemma is now clear for all to see, and the battle lines have been drawn, with the government and technology industry taking dueling views on the way to proceed. FBI Director James Comey has argued that the increasing availability and use of endpoint and end-to-end encryption puts our country at grave risk, as it effectively creates safe spaces for criminals and terrorists to operate outside the reach of law enforcement or the Intelligence Community. He acknowledges the important privacy interests at stake, but asserts that those interests must be balanced with the security interests of the broader society and urges industry to search for a technological solution that can accommodate the government's lawful surveillance needs.

Representatives of the technology industry and the civil liberties community have aggressively countered Director Comey's position with a variety of arguments, including the following:

- That any accommodation for the government would introduce a vulnerability that would undermine the security and integrity of encryption, which inarguably is a vitally important technology for protecting information and preventing theft and other cyber mischief;
- That any such accommodation could not be confined to the United States, as other governments—including repressive governments—would likely demand the same access;
- That any accommodation would put U.S. technology companies at a competitive disadvantage because customers—especially overseas customers and those who are already suspicious of U.S. Government surveillance in the aftermath of the Snowden revelations—may stop using those companies' services if they learn that the companies are cooperating with the U.S. Government to circumvent encryption; and
- That any accommodation imposed on U.S. companies would be of limited effectiveness because criminals, terrorists and other wrongdoers would simply start using foreign encrypted services.

Citing these arguments, some in the technology industry and civil liberties community have taken an absolutist position that there should be no government ac-

commodation at all. One technology industry association sent President Obama a letter urging him to resist "encryption 'work-arounds'" for the government's surveillance needs, contending that a work-around would "compromise the security of [communications] products and services, rendering them more vulnerable to attacks and [] erode consumers' trust in the products and services they rely on for protecting their information."

I fully appreciate the importance and tremendous societal value of strong encryption, and I recognize the validity of the technology industry's concerns. However, I do not believe that those concerns automatically mean that encryption should be inviolable and that our Government should henceforth be denied access to large swaths of communications. That reasoning just does not square with the reality of today's national security imperatives.

That reality is that government access to these communications is critical to our national security. From my earliest days as a federal prosecutor investigating narcotics networks, I saw the value of communications surveillance in gaining insight into the plans and inner workings of a conspiracy. That value is particularly high when the conspiracy being investigated is a foreign terrorist group, where leaders and foot soldiers are often located in different parts of the world and have to rely on electronic communication for operational coordination.

Thanks in large part to our signals intelligence capabilities, the government has been fairly successful in detecting and protecting our country against large-scale terrorism since 9/11. That record of success is now being tested, however, by the rise of ISIS, which in many ways is a more formidable adversary than al-Qaeda ever was. In response to our allies' recent success in pushing back the borders of its conquered territory, ISIS seems determined to counter those losses with terrorist attacks directed against the homelands of those countries—like the U.S.—that they consider their mortal enemies.

It is also clear that ISIS recognizes the operational value of encrypted communications. We know that it has issued a guide for its members discussing the relative "safety" of different encrypted messaging apps. We know that as part of its recruiting efforts, ISIS often initially engages on social media, but then moves the conversation to encrypted apps. We know that attackers inspired by ISIS have made use of such apps prior to conducting their attacks. For example, FBI Director Comey has testified that one of the attackers at the Muhammad art exhibit in Garland, Texas exchanged over 100 encrypted messages with a known overseas terrorist on the morning of the shooting. Those messages remain encrypted and unreadable by investigators.

V.RESOLVING THE DEBATE

With this gathering threat on the horizon, now is not the time to blithely concede that encryption automatically trumps surveillance and allow our intelligence and law enforcement agencies to go dark. To the contrary, now is the time for Congress to mobilize on this issue and push for a solution—a solution that allows government the access it needs to protect our people and our country without unduly compromising the encryption technology that protects our data and communications.

I urge Congress to embark on a legislative process that calls on both sides of this debate to fully lay out the basis of their views:

- For the government, this means laying out the case that concretely demonstrates how significantly their different investigative efforts are—or are not—handicapped by the use of default encryption technologies.
- For the technology industry and civil liberties groups, this means laying out technically specific support for the contention that a government accommodation would undermine the integrity of default encryption. They should provide hard data that demonstrates exactly how—and how much—each possible type of accommodation would impact their encryption systems. It is only when Congress receives that data that it can knowledgeably perform its deliberative function and balance the potential cyber security dangers posed by a government accommodation against the national security and law enforcement benefits of having such an accommodation in place.

Congress can undertake this effort either through a series of hearings and a traditional legislative process, or else through the establishment of a commission like that proposed by Senator Warner and Chairman McCaul—a commission composed of technologists, security experts and other key stakeholders who could delve deeply into the intricacies of this complex issue.

Either of these options would be a significant step forward. The option that is not a step forward is the option of inaction and continued impasse. We have seen the consequences of that option before, as that was the option the government effec-

tively pursued in the late 1990's and early 2000's when debating the wisdom of "the wall," the regulatory barrier that prevented coordination and information sharing between law enforcement and Intelligence Community personnel. That inaction had tragic consequences when the existence of the wall contributed to our inability to identify the 9/11 hijackers and prevent them from launching their attacks.

Congress dismantled the wall when it passed the PATRIOT Act six weeks after the 9/11 attacks, but that was too late for the 3,000 murdered Americans. We made the mistake of inaction once before; we must not make it again.

I applaud the Committee for holding today's hearing and showing leadership on this issue. It gives me hope that we can, in fact, move beyond the current impasse and reach a workable solution to this critical problem. My thanks again for inviting me, and I look forward to answering any questions you may have.

Chairman MCCAIN. I thank you. I want to emphasize to you, sir, that I view this issue as one of the most compelling for a whole variety of reasons, and I intend for this committee to, if necessary, take up separate legislation to try to address an issue that has clearly not been resolved.

Mr. Vance, we, Republicans and Democrats, liberals and conservatives, disagree on a lot of issues. One issue we do not disagree on is the horrible crimes that are committed by child pornographers and human traffickers. I know of no one that does not condemn this terrible, terrible exploitation of the innocent in our lives and our society.

What we are doing here, if you would mention again, we are basically protecting child pornographers and human traffickers. We are protecting them by giving them access to encrypted mechanisms so that they can carry on their disgraceful, odious conduct.

I guess I say that because we talk about encryption and freedom of speech and government intervention and all that, but I thought one of the fundamental requirements of any government is to protect the defenseless. Now, de facto, by this encryption and failure for us to allow law enforcement people such as yourselves to have access to this information, we are furthering the cause of child pornographers and human traffickers.

Your comments, Mr. Vance?

Mr. VANCE. Senator, I absolutely agree that the consequence of this device default encryption, which was a purposeful reengineering of the devices to make them inaccessible and to be unlocked even with court order, the consequence of that is a loss of, speaking for local law enforcement, local law enforcement's ability to do the job that each of us was sworn to protect.

The cases that we outlined in our white paper from November 2015 described to the committee some of the absolutely horrific fact patterns that in the past we have been able to solve those issues because of access to devices. As I say, in our office alone, there are 314 cases ranging from murder to child sex abuse that we can now not access those devices.

The answer is yes. I think, from my perspective, Senator, the reason I think this is so important, that the legislature deal with this, and why I am so grateful that you are giving further visibility to this, is that it seems to me that there are some in the technology community who have come to the conclusion that the inability to find a path toward justice for victims in the cases that I described is simply collateral damage and acceptable collateral damage in the service of their privacy position.

I, for one, have a hard time understanding how I can explain that to the victims of crime in my community.

Chairman MCCAIN. Even though the United States Supreme Court, if I recollect, stated that child pornography was unique in itself and its criminal activities. "I know it when I see it" is one of the phrases that was used.

Twitter barred a data miner, a company specializing in searching across millions of tweets to identify unfolding terror attacks and unrest, from accessing its real-time stream of tweets because of its work for U.S. intelligence agencies.

What are your thoughts, all three witnesses, on Twitter's decision to ban this valuable counterterrorism tool from being used by the intelligence community, even though Twitter continues to sell the information used about consumers for a profit?

Mr. Inglis?

Mr. INGLIS. Sir, if I might, I will answer that question, and first go back to the previous question.

I fully support the comments made by Mr. Vance about the nature of the choices being made with respect to the use of default encryption. The idea that the private sector believes that they are the arbiter of that choice is both inappropriate and I think unnecessary because I do not think we have to choose. I think that are systems that we can develop that essentially deliver appropriate security for those systems.

He gave a great example between operating versions seven and eight, and that at the same time can deliver appropriate access for the government when and where it needs it.

Chairman MCCAIN. Is that a second key idea?

Mr. INGLIS. Pardon, sir?

Chairman MCCAIN. A second key?

Mr. INGLIS. There are any number of schemes that you can bring to bear. That might be one of them. I think the government is taking great pains, and I think appropriately so, to not specify an implementation because I would defer to the innovation of the private sector which has shown——

Chairman MCCAIN. If they want to, they could.

Mr. INGLIS. They could. They could.

There are any number of ways that you can do this and that you could provide appropriate protection for that, without giving the government the keys to the store or, for that matter, rogue governments that might want to have access to the same thing.

To your question about the data miner, I think it is inappropriate and hypocritical for a data miner to retain that information for use for commercial purposes, but not to provide that such that society, writ large, might be protected.

Chairman MCCAIN. That is Twitter's fault, right, because Twitter stopped doing business with them? It was kept from accessing their real-time stream of tweets.

Mr. INGLIS. Senator, I do not disagree. The shame of the larger proposition is that, increasingly, entities within the private sector stand in as the arbiter of how you align these societal values. I think that is not appropriate.

Chairman MCCAIN. I see.

Mr. Wainstein?

Mr. WAINSTEIN. Thank you, Mr. Chairman. I agree with Mr. Inglis on this issue.

I would like to point out the broader question or the broader concern that I have, which is just generally about cooperation by private industry with our efforts to protect the country. As a prosecutor for 15 years or so, I enjoyed great cooperation from most of the telecommunications providers and others in the industry. When we were running down terrorists or criminals, they were very helpful.

I think there has been a change since the disclosures by Snowden, and I think there are now business reasons for some companies to not only scale back on their cooperation with the government, but to be seen by customers and potential customers as scaling back because they think there is a business disincentive for them to be seen as cooperative. There are some customers who will go to other companies if they think that your company is being too cozy with the U.S. Government.

That is terribly unfortunate. I think part of what I would like to see come out of this legislative process, which you just discussed embarking on, is the clear signal that we expect cooperation and we should have a cooperative relationship.

This is not to say there isn't. I was briefed recently by a major technology company that is doing a lot of really good stuff for the intelligence community, so there is cooperation going on. I just think it is very unfortunate that some companies are resorting to these public measures to show how they are distancing themselves from the U.S. Government.

Chairman MCCAIN. Well, I am reminded when the technology companies say that, well, other countries will not do business because of the fact that there is a possibility of compromise, I am reminded of when, after the scandals of the 1970s, we enacted antibribery laws and everybody said, oh, no, you cannot do that because then these countries will not do business with our defense companies and corporations. That obviously did not happen.

My time has long expired, but I do think it is important to point out, and maybe we can get a comment later on, there is a Wall Street Journal article that says, "How Islamic State Teaches Tech Savvy to Avoid Detection." It is a well-known fact that Mr. Baghdadi is sending people into the refugee flow with encrypted phones in order to carry out acts of terror. That is well-known. It is not classified information. Yet our technology companies seem to be ignoring that direct threat to the security of the United States.

Senator Reed?

Senator REED. Thank you very much, Mr. Chairman. Again, thank you for holding these hearings. This is the second. There will be many more, because this issue is extraordinarily complex.

I do not want to oversimplify it, but let me suggest, at least to begin, that there are two perhaps distinct issues here, among many. One is a phone that law enforcement authorities physically have in their custody. The question is, should there be a statute that gives the right, or demands the company gives you access to that phone? That seems to me more straightforward than the second issue, which is how you access encrypted communication before

a crime or with probable cause that a crime has been committed, but you do not yet have a complete case.

Mr. Vance, are there technological ways to do that that the companies could provide? That is the first issue here, too, in terms of getting into that encrypted——

Mr. VANCE. On the phone itself?

Senator REED. No, I am talking about one of the challenges we have, particularly to anticipate criminal activity, to investigate it, the old wiretap, where you had probable cause to suspect a crime was being planned, went to a court. In the old days, you just put the electrodes, the wires on the phones, and you were listening in and you got information. Can we physically do that now, technologically?

Mr. VANCE. Senator, in our office, we have historically used title III to access data in transit, cell phone to cell phone, text to text. It historically has been doable.

Obviously, the developments of encryption software, purposefully, in some cases, directed to be used by outside terrorism actors, affects that. Director Comey, I think, has been the most powerful spokesperson on that interest.

Going forward, the answer to your question is, can you create an environment in which law enforcement, pursuant to a court order, can access communications and others cannot? That is the technological question that I think all of us are struggling with.

I would suggest that, and, respectfully, the answer has to be yes. We are an enormously creative and innovative country with geniuses in the technology community, as well as in the security industry, particularly at the Federal level. I find it not a solution for industry to fold its arms and say we are not going to provide any way forward for this debate. I think that is not helpful. I believe that, surely, with all the other technological advances we have achieved, this is not impossible. It is just not being—there is no direction or requirement that this be addressed by the technology industries and the government in a coordinated manner.

Senator REED. Again, my knowledge is not as extensive as yours. That will require not only the makers of the phones but the Internet providers to be able to, pursuant to court order, have the means of getting into the phone surreptitiously, because you do not want to disclose your activities, and extracting information.

Mr. VANCE. I think that is accurate. Again, though I am not the smartest technological person in the room, I think that does not mean that it is not achievable.

Senator REED. No, I think the technology could be there. I just want to make sure we are focused on what has to be done, and then let people to it. That is the issue of end-to-end encryption.

I second Mr. Wainstein's comment, too. I think after Snowden, there is a whole different attitude in the industry about this, and there are business considerations about who is the most secure, et cetera. I think it was a very interesting and important point to make, Mr. Wainstein. That is something we have to face going forward.

Just to the whole panel, I mentioned in my opening remarks Secretary Chertoff, Admiral McConnell, very distinguished, thoughtful

people who spend their lives dedicated to national security, have taken a very different position, saying several factors.

First of all, these are real problems but there is a greater issue, and that is protecting legitimate information from cyber intrusion. That is one aspect.

The second aspect is that, and the chairman alluded to this, that if we do it, and the rest of the world does not do it, we are at a disadvantage.

Third, we tried efforts to control encryption technology through legislation before, and they have not worked.

Quickly, my time is expired, but I will start with Mr. Wainstein, your comments?

Rebuttal, Mr. Vance and Mr. Inglis?

Thank you.

Mr. WAINSTEIN. Thank you, Senator Reed.

First, that list that you just read off of people are some of the finest public servants this country has ever had, and they are close friends and colleagues of mine, and I have tremendous respect for their opinions. They raise good points.

As I said in my remarks, there are strong arguments on the technology industry side of this. There are real concerns, and they have raised them.

I guess my response would be this. Those concerns have been raised, and there have been arguments as to why this might end up unduly compromising encryption, which really is an important thing for society.

The only way you are going to be able to do your job and balance the need for an accommodation against the impact it might have on encryption is for them to show exactly, specifically, technically, how that damage would come about.

This potential, whether it is escrow key accommodation or another one, look at that and have them lay out exactly what that will do to encryption that causes them concern.

We have not heard that yet. Until we hear that, you cannot do your job and come up with a solution.

Senator REED. Thank you very much.

Mr. VANCE. Senator, I could not agree more with what Mr. Wainstein has said. In fact, I think it has been one of our frustrations that there has not been the ability or the willingness to quantify the increased loss of security.

Now, as I indicated, we just learned recently that it appears that there had been no data compromises by virtue of phones running on iOS 7 being open pursuant to court order. I think we all, listening to the technology community, thought that this was happening all the time. The fact of the matter is, it turns out it was actually extremely secure.

I think there is reality and then there is argument and advocacy.

As to the international disadvantage, I certainly think we need to take that seriously, but I think it is safe to say that the world has found a way to address the individual requirements of each country in the world to respect their sovereignty.

If Volkswagen or any company wants to sell a car in the United States, they have to meet certain security standards—in some way, or at least—really, really meet them.

Chairman MCCAIN. Bad example.

Mr. VANCE. That is not a strange concept in the world of international commerce. If governments want to move money in and out of treasury departments around the world, there are certain standards that are required in each country before money is accessed and moved.

This has happened before. It is not a foreign concept to the world.

Senator REED. Thank you, Mr. Vance.

Mr. Inglis, please?

Mr. INGLIS. First, I support the remarks of the prior two speakers. I absolutely have an enormous and abiding respect for the individuals that you cited who made that comment.

I would say the following. First, if the choice is to weaken security, such that the government or others might have access to it, or to leave it strong, of course, the right choice is to leave it strong. I do not think that is the choice. I think that is a false choice.

Second, I would observe that there are a variety of circumstances under which, as a desired feature, we cut a third party into a conversation, maybe for a teleconference purpose or because you want to blind courtesy copy somebody on an email. For a variety of purposes, we essentially do software upgrades because we want to patch a system, and we have the means by which, from the vendor to the devices at the edge, we can have a sweeping application of software.

We do not call the former a backdoor, and we do not call the latter a secret method to denigrate the quality of the software. We call them features. I think the technology exists such that we might do this.

To the comment that if we set this up, other foreign governments might then misappropriate it, that is a real issue. I think that we need to think our way through that. If we do not drive the rules, they will.

There are thoughtful nations, like the United Kingdom United Kingdom, that are thinking their way through this, and they have come up with something in the investigatory powers bill, which I think is likely to be passed this fall, which is going to strike an alignment, not a compromise, but an alignment of these great goods. There are other nations that will not be as thoughtful as that.

If the United States stands by, we defer to the wishes, to the values set, of others. If we lead, we might just perhaps drive that to the place we want it to go.

Senator REED. Thank you very much.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Cotton?

Senator COTTON. Thank you, gentlemen, for being here on this important topic.

I speak today as a friend of encryption, someone who recognizes its vital role in protecting some of the most important data that we all have, whether it is our email, text messages, phone calls, health information, financial information. Also someone who wants to protect the American people, to protect them from mass casualty terrorist attacks, to prevent them from being shot in nightclubs or in

community centers, or blown up in malls, something that is as important if not more important than protecting that data.

I also recognize the great contribution that companies like Apple and Twitter and Facebook have made to our society and the way that we live today.

I hope that there is some way that we can all find some compromise or alignment, as Mr. Inglis called it, to address all of these threats to the American people.

Mr. Inglis, I want to touch on a point you just made. In this debate, we often hear a lot about backdoors. As you said, many companies employ software update mechanisms that could be thought of as a backdoor because they change or update the functionality of the device periodically, and sometimes without even notice.

These require additional keys or pathways to enter a device, so could you elaborate a little bit on, if a company can build a safeguard or additional key for updates and patches, why they could not do so for safeguards or keys for emergency purposes like terrorism, like kidnappings, like child pornography and so forth?

Mr. INGLIS. I think your point is well-made, sir. I think that they can.

The question is not whether that capability exists or not. It certainly does exist, that you can upgrade software, that you can add other parties, legitimate parties, at the behest of the user to conversations, whether it is retraction to pull stored data, or whether it is a conversation in motion.

The question is, is there a legitimate purpose that we understand and say that is sufficiently noble, we are going to engineer the solution. Do we have the controls on that, such that we are confident it will be used for that purpose and no other.

It is the bookends, not the capability, that then should be the focus of our conversation.

I think the technology does exist. The question is whether we can engineer that and have confidence about its efficacy.

Senator COTTON. Let's put this question in a bit of a broader societal and legal context, Mr. Vance. We all have an expectation of privacy in our bank accounts, of course. However, you, I would assume, regularly obtain lawful subpoenas from a court to obtain the bank records of someone suspected of engaging in criminal activity. Is that correct?

Mr. VANCE. Correct.

Senator COTTON. We also have reasonable expectation of privacy in our telephone conversations, the actual content of those conversations. However, I would assume that you often seek court-ordered wiretaps from telecom providers when there is a reasonable suspicion of criminal activity?

Mr. VANCE. Correct.

Senator COTTON. Is there any reason why technology and data companies should be treated differently from banks or telephone companies in our society?

Mr. VANCE. Senator, I believe there is no legitimate objective reason. I think what is interesting about the state of affairs we find ourselves in today is, sticking with Apple for a second, they reengineered the phones so they can no longer be opened by the company. That was a conscious choice.

Having done that, they have now argued that they have created a right to privacy that previously did not exist because of their engineering decisions to block access by law enforcement.

I think that is ironic, but that is where we are today. I find no logical, reasonable reason why the technology companies should not be subject to the same sorts of rights and obligations that other industries have come to adapt and have worked through over the decades. I think that is something that is fair to look at going forward.

Senator COTTON. Mr. Wainstein, do you have any perspective on whether there should be some special set of rules for technology and data companies, as opposed to banks or telephone companies?

Mr. WAINSTEIN. No, Senator Cotton. Look, I agree with Mr. Vance on this, that as a sort of our compact with our Government, we all, individuals, industry, companies, we have to submit to lawful court orders.

Despite this encryption, as Mr. Vance said, they did not create a new zone of privacy. They cannot do that. The privacy is as dictated in the Constitution and by the decisions of our courts.

They have an obligation to provide that information. They have tried to litigate it. At the end of the day, I think they are going to lose on the fundamental issue. I am quite confident they will. I think that it is really up to Congress to make the point legislatively that unless you voluntarily accept the solution to this, it is of such paramount importance to the national security and to enforcement of our laws that we are going to legislate it.

Senator COTTON. We all have certain rights to privacy under our Constitution, but we also have a duty to provide information when subjected to a lawful court order, and that would be a duty not to our Government, but to our fellow citizens.

Thank you.

Chairman MCCAIN. Senator King?

Senator KING. I think it is important to clarify, because there is a lot of confusion in this discussion, even in this hearing.

Encryption, the encryption horse is way out of the barn. We are not talking about encryption. We are not talking about WhatsApp or Telegram. That is done. It cannot be broken.

We could say WhatsApp, you are owned by Google, you have to open it up. Somebody goes and buys Telegram, which is from Germany, and the Internet as a free exchange across borders.

I mean, if NSA can break it, that is one thing. I do not think any of you are suggesting, or are you, that somehow we can deal with the encryption of apps that al-Baghdadi is using.

I think we need to clarify this discussion. We are really talking about the Apple case and compelling technology companies to provide access to their devices.

Am I not correct? Encryption, that is a done deal, isn't it?

Mr. INGLIS. I think it is, sir. It is a done deal. It is a good thing that encryption is in wide and almost ubiquitous use.

Senator KING. That is not really the question before the house. The real question are issues like the Apple case.

I think one of the problems we have to think anew here is, is that this is an international phenomenon. It is not neat borders, sovereignty. It is very difficult to make those things stick where

you have something that moves invisibly through the air and can be built anywhere in the world. It seems to me that is one of the problems.

We could pass a law here that forced Apple in some way, shape, or form to provide the key to open their iPhones. Whether or not that law would apply to an iPhone made in Turkey or Germany or Russia—and I guess we could try to pick them up at the border, but it is like squeezing Jell-O. I mean, it is going to be a very difficult technological—the international aspect of this makes it incredibly more difficult.

Mr. Inglis, don't you agree?

Mr. INGLIS. I do agree, sir. I think that, then, this government has a dual obligation. One, to figure out what our values are such that we would drive choices to be biased toward an alignment of these, as I described it, four interests. It could be that it is three interests. At the same time, work with like-minded governments to create an international regime where it is more likely that these products will win in that marketplace and put our vendors in the right position.

Senator KING. I agree with that. This is a very difficult issue to grapple with, because basically we are balancing two provisions of the Constitution, provide for the common defense and ensure domestic tranquility, and the First, Fourth, and Fifth Amendments. I mean, that is what we are trying to do here.

I do not like commissions, but I signed on to Senator Warner's bill to set up a commission to really look in depth at this issue involving the technology community, the law enforcement community, and the intelligence community, and come back to us with some really good thinking. I like your term of alignment.

As I say, I do not generally—I think commissions often are a copout. I think in this case—and I totally agree that this should be a legislative solution. It should not be case-by-case in various Federal district courts. It should be a legislative solution. It is a policy issue.

I think we need more information, frankly. I commend the chair for setting up this hearing, but I think this really needs some deep thought by a lot of people because it is really, in many ways, new territory.

Mr. Vance, hypothetical, and I know we were all taught in law school to never ask a question you do not know the answer to, and I do not know the answer to this.

If a locksmith makes a safe, and it is set up in such a way that the customer can set the combination and the locksmith does not know the combination, cannot open it, could you get a subpoena or a warrant to force that locksmith to somehow break into that safe?

Mr. VANCE. We would, Senator, likely get a warrant permitting us to, through physical force, open that safe with court directive.

Senator KING. That is my point. The FBI found a way to get into the Apple iPhone. They did not make Apple do it. In your answer, you just conceded that you would not make the locksmith do it. You would figure out how to do it.

One of the things, frankly, that really bothered me about the Apple case was that we had all this excitement and publicity about a great American company that went on for months and months,

and then the FBI said never mind, we figured out how to do it. That bothered me.

They should have exhausted all of those remedies before they went to that magistrate in California and said we need something under a 200-year-old All Writs Act.

You couldn't enforce that locksmith to come in and somehow break into that safe.

Mr. VANCE. Senator, I think that legislation could be passed which would require that locksmith to have the ability to open that safe, if we reached a level of volume, such as we are reaching right now with the probability of a problem getting into encrypted devices that are relevant to law enforcement investigations.

Senator KING. You have 300 cases pending, so this isn't about one iPhone in San Bernardino. You have 300. Where does it stop? Is this for an OUI [organization unique idenfier] in Poughkeepsie that you are going to be able to open the iPhone? Is there any limit? Once we say law enforcement can get a warrant to force Apple or Google or whoever it is to open their phone, is there any limit on that?

Mr. VANCE. I am not sure why there would be any other limit than the constitutionally recognized requirements of a court-ordered, specific warrant based on probable cause. Yes, if that standard was met in Poughkeepsie or New York City or California, that warrant should be able, in my opinion, to be affected.

Senator KING. I think that is a very important point, because a lot of the publicity and discussion and testimony at the time of the original San Bernardino case was we only want this for one phone. We are not talking about one phone. We are talking about thousands of phones.

Mr. VANCE. I am certainly not talking about one phone, Senator, absolutely. I believe it is because we are talking about thousands of phones that represent criminal investigations involving thousands of victims and investigations that may relate to security beyond the individual victims, that is why it is so important that this committee has taken this issue up and is looking at it with an eye toward potential Federal legislation.

Senator KING. One quick question, Mr. Chairman.

Do you fellows have any few on the Warner bill on the commission idea?

Mr. VANCE. Senator, my view is that a commission sounds like a very sensible, thoughtful thing. As I said before, there is a sense of real urgency, particularly in State and local law enforcement, that we reach a resolution that could permit us to go forward.

It is 1,000 cases. Maybe it is 5,000 cases around the country. Each of our cases in State court have statute of limitations, once filed, that we are operating under. We have victims of real crimes that are waiting for justice all around the country.

If a commission was a commission that went on for 18 months and that issued a nonbinding recommendation at the end of that 18 months, from this one prosecutor's perspective, I am not sure that addresses the urgency with which State and local law enforcement need to deal with this problem.

Senator KING. Mr. Inglis?

Mr. INGLIS. I largely agree with all of that.

It might well be that the government's best play is to say that it intends to act to create a stalking horse with a sense of urgency, but, at the same time, it intends to do so in the most thoughtful way and the most well-informed way possible, such that then the commission creates an opportunity to establish a venue at which a very diverse array of disciplines, functions, perspectives, then can come together, but to encourage collaboration in advance of what ultimately will be a government action.

There is an urgent need to get on with that, and thus far we have not seen the kind of collaboration required to bring the diversity that America has been so well-known for to the table to pull that off.

If I might go back to your earlier question, I think you are quite right to raise the context of the All Writs Act. Leaving aside, which I think you are right about the precedent of one versus a thousand, I would say that I think we are likely to find that the All Writs Act is insufficient, that it was not imagined it could be used in this situation, and, therefore, Congress needs to act to actually update that and bring that into the modern age.

Two, with respect to the San Bernardino case, the idea that in the absence of an All Writs Act, the absence of an ability to compel the vendor to assist, that you then turn to the FBI and say you are just going to have to hack the civilian infrastructure, I think that puts the government in exactly the wrong place. You do not want government hacking civilian infrastructure, the private sector's infrastructure. You want government aiding and abetting the increased resilience of that infrastructure.

You, therefore, need to figure out how upfront do I attend to all of government's responsibilities to provide for collective security, which is what Jim Comey is pursuing. That is his lawful charge. At the same time, have deference and support for the individual privacy and security that is attendant to the Constitution's promise.

Senator KING. Thank you. Thank you for your thoughtful testimony on a very tough issue. I appreciate it.

Chairman MCCAIN. If we did a commission, it would be at least a year, at best. The point is this issue is not so complicated.

We have banking laws in the United States that are not respected by every country in the world, but we enforce them because anybody who wants to do business with the United States of America has to abide by those laws. We have other rules and regulations that we enforce—antibribery—that other nations engage in.

We set the pace, and we are the ones who dictate the terms because we happen to be the largest market in the world.

I have heard this song before about, well, other people are going to do it. Therefore, we should not do it. I do not accept that argument.

When we have child pornographers who are operating freely—freely—and human traffickers who are operating freely, there is an urgency to this issue, which is why this committee has taken up, and is going to have more hearings on it, including hearing from the technology companies, even if they do not want to come here. This committee has subpoena power.

For them to blatantly say that they will not give us information or give us the ability to acquire information as we have, as you pointed out, Mr. Vance, on banking financial records, all kinds of other ways that we have of pursuing criminal activity, but somehow this new technology should be exempt from all of that is something that I do not buy. Nor do I think the families of those young girls who are being human trafficked right now, nor those children who are now the victims of child pornography, which is being protected by the way that these companies are doing business now. I find it unacceptable.

Senator Blumenthal?

Senator BLUMENTHAL. Thanks, Mr. Chairman.

I want to thank you for those comments. I share those concerns about the power of our private sector, financial and communication companies, that have immense financial and market power, and the ability to do good and cooperate and protect victims of human trafficking, as well as of terror, extremism, and violence.

The United States is home to some of the world's leading social media, advertising, film, communications companies. One of ISIL's most powerful tools for recruitment is its social media campaign. The group releases absolutely horrifying but expertly done videos inspiring young people to join its ranks.

On the one hand, our modern, interconnected world gives ISIS the ability to reach the United States, no matter how robust the physical barriers or boundaries may be. On the other hand, their hatred for us is absolutely inescapable and open, and we need to intensify our efforts against those malicious messages, including forging solidarity with the Muslim world, which has as much to lose as we do. The messages of intolerance and persecution and extremist violence I think can bring us together, even as our adversaries and enemies seek to divide us.

I want to thank all of you for being here today on this supremely important topic, particularly District Attorney Vance.

Thank you for your good work. I know of all of your distinguished service.

District Attorney Vance happens to work in a venue close to my State of Connecticut in an area where I used to work as well, both as a Federal prosecutor and as State Attorney General.

I think your work is supremely important in this area, and your leadership and advocacy.

I want to ask a question that is directed to the private sector.

How can we bring the private sector to cooperate more closely and be a better partner of law enforcement in this area?

Mr. VANCE. I am not expert in these matters, but I do think, as I was saying, Senator, that whether the private sector is willing to acknowledge it or not, this is an urgent issue. It is urgent because it is affecting national security, about which I am not an expert, but local security, about which I have some knowledge.

Now I guess the commission, a presidential commission or congressional commission, is one sure way to start the process. One of the Senators has suggested that.

I think it needs the active involvement of the administration. I think the President and his administration needs to grab ahold of the collar of local law enforcement and the enforcement commu-

nities, grab ahold of the collar of the private sector, pull them into a room, work at an accelerated speed with an eye toward getting a resolution to this or some recommendations on how to go forward between now and the end of the year.

That may be totally unrealistic from a calendar standpoint with the way we are in America right now, but unless the administration is going to come in and assist the Congress, local law enforcement and others, I think it is not going happen.

Senator BLUMENTHAL. Yes, sir?

Mr. INGLIS. Sir, I would add to that that I think the government first and foremost, Mr. Vance's point, needs to indicate its desire to lead, its intent to lead, as opposed to observe.

Then second, the framing will be profoundly important. If the government were to approach this by saying we intend to impose a requirement on the private sector, to satisfy Mr. Vance's or perhaps Jim Comey's need for exceptional access, that is one way of framing it.

Another way to frame it would be to say that we intend to guarantee or to align the kind of collective distinguished interests that are on the table here, kind of individual pursuit of security to include companies' abilities to innovate and succeed in national, international marketplaces, and the ability of governments when necessary under exceptional access to access communication for purposes of what Mr. Vance and Jim Comey are pursuing under their lawful mandate. That is a very different framing.

That might then encourage people to say I am coming to the table because that is the way we are essentially going to make a contribution against the interests I am charged to represent.

Senator BLUMENTHAL. What I see, from Connecticut's standpoint, and we have very able Federal prosecutors, our United States attorney, Deirdre Daly, whom you no doubt know, Mr. Vance, as well as our State prosecutors, increasingly tell and show me that our local and State security are inseparable from our national security, and that the bad guys have seamless ways of accessing information and communicating with each other, and we remain separated in terms of our law enforcement jurisdiction and our inability to access the very means of communication that they use so seamlessly.

I share the chairman's and your sense of urgency, not that I oppose a commission. Who could oppose a commission focused on this issue? I feel a much greater sense of urgency and immediacy about the need to address these concerns.

Thank you very much, Senator Reed, Mr. Chairman.

Thank you to our panel.

Senator REED. [Presiding] On behalf of Chairman McCain, let me recognize Senator King for a very quick question, because we have floor activity.

Senator KING. We have to go vote.

I just want to again sort of clarify. You can tap phones now, right, Apple iPhones, if you get subpoenas, Mr. Vance? You can get the verbal conversation?

Mr. VANCE. Some, unless the communications, for example, are encrypted.

Senator KING. Okay. Okay, but encryption, we talked about encryption. Encryption is not the issue here. Encryption is encryption, and you can either can get it or you cannot.

You can get messages. You can get the content of messages, unless they are encrypted. You can get where people called under the 215 program under the metadata.

I just want to be clear what it is you can already get without asking companies to unlock their phones, because you are really talking about something other than phone calls, messages, and metadata. You are talking about maybe the geographic—anyway, I just think it is important.

That shows the complexity of this issue. You have to really do it in a granular way.

Mr. VANCE. Senator, I understand what you are saying. Let's just talk about data at rest, which is of the most interest to law enforcement of what is on the phones. Interestingly, many criminals do not encrypt, and that was one reason why we were able to get so much information about rape, robbery, murder, and other state law crimes.

Why they do not encrypt is a question I cannot answer. The fact of the matter is that even when there has been encryption technology, it is not used by the vast majority of people committing crimes.

Therefore, there is an absolutely direct consequence because of now our inability to access those phones, with a court-ordered warrant, information that is on the phone likely not to be encrypted relevant to the criminal investigation is inaccessible.

Senator KING. I understand. I would appreciate, to the extent you guys can give us suggested language or proposals or outlines of legislation, that is what we are looking for. Thank you very much.

Thank you, Mr. Chairman.

Senator REED. Thank you, Senator King.

Gentlemen, thank you for your extraordinarily thoughtful testimony. I can assure you that as the days go forward, and you made it quite clear this is not something that can take forever, we will be reaching out for your advice and your assistance.

I second Senator King's point. Any proactive legislative proposals or ideas, please forward them.

On behalf of Chairman McCain, I also want to explain that this is a busy day, lots of floor activity. Your testimony was extraordinarily important, the most important issue that we are coming to grips with, which is cybersecurity and protecting the Nation. My colleagues were, I think, deflected to the floor, so I apologize.

Let me thank you all for your extraordinary testimony. On behalf of the chairman, Chairman McCain, let me adjourn the hearing. Thank you.

[Whereupon, at 10:55 a.m., the hearing was adjourned.]

ENCRYPTION AND CYBER MATTERS

TUESDAY, SEPTEMBER 13, 2016

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:37 a.m. in Room SH–216, Hart Senate Office Building, Senator John McCain (chairman) presiding.

Committee members present: Senators McCain, Wicker, Fischer, Cotton, Rounds, Ernst, Sullivan, Lee, Cruz, Reed, Nelson, McCaskill, Manchin, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, King, and Heinrich.

OPENING STATEMENT OF SENATOR JOHN MCCAIN, CHAIRMAN

Chairman MCCAIN. I would—since a quorum is not present, but we have pending military nominations, I would ask unanimous consent to waive the requirement for two more members in order to conduct a routine business for the 4,158 pending military nominations, which I'm—none of which are controversial. Is there any objection to that?

[No response.]

Chairman MCCAIN. If not, since—a quorum is not present, but I ask the committee to consider a list of 4,158 pending military nominations. Of these nominations, 503 nominations are 2 days short of the committee's requirement that nominations be in committee for 7 days before we report them out. No objection has been raised. These nominations—I recommend the committee waive the 7-day rule in order to permit the confirmation of the nomination of these officers before the Senate goes out for the October recess.

Is there a motion to favorably report these 4,158 military nominations to the Senate?

Senator REED. So move.

Chairman MCCAIN. Is there a second?

Senator Wicker: Second.

Chairman MCCAIN. All in favor?

[A chorus of ayes.]

Chairman MCCAIN. The motion carries.

I thank the committee. We wouldn't want to go out for a long period of time with these pending nominations, none of which are in any way controversial.

I think that there was a cyber attack on Admiral Rogers' automobile, which accounts for him being late this morning.

[Laughter.]

Chairman MCCAIN. We'll have a full investigation——

Voice: He's joking.

[Laughter.]

Chairman MCCAIN. Mr. Secretary, we welcome you and Admiral Rogers. We'll begin with you, Mr. Secretary.

Mr. LETTRE. Chairman McCain, Ranking Member Reed, members of the committee, thank you for inviting us to discuss the importance of strong encryption, trends on its use, and its impact on the Department of Defense.

With your permission, I've submitted a longer written statement, and I would ask that it be made part of today's record.

Chairman MCCAIN. If you'll hold for a moment, Secretary Lettre, in my—I forgot the opening statements by myself and the Ranking Member——

[Laughter.]

Mr. LETTRE. I was wondering about that.

Chairman MCCAIN.—which is the reason why so many of my colleagues are staying here, in order to hear our words of wisdom.

[Laughter.]

Senator NELSON. We thought you were going to spare us.

[Laughter.]

Chairman MCCAIN. Probably should, given the calendar, but could I just—I'll go ahead, Secretary Lettre.

Encryption has become ubiquitous across the counterterrorism fight. The Islamic State of Iraq and the Levant [ISIL] has successfully leveraged messaging applications developed by some of our most innovative companies to create an end-to-end encrypted safe haven where they can operate with near perfect secrecy and at arms' length of law enforcement, the intelligence community, and the military. From Syria to San Bernardino to Paris to Brussels to perhaps even Orlando, ISIL has utilized encrypted communications that, just a few years ago, were limited to a select few of the world's premier military and intelligence services.

As I've stated in the past, this is a complex and difficult problem, with no easy solutions. We must balance our national security needs and the rights of our citizens. We must also recognize that authoritarian regimes are eager to gain keys to encrypted software so they can further their own abusive policies, such as suppressing dissent and violating basic human rights. Yet, ignoring the issue, as the White House has done, is also not an option.

I look forward to hearing how the use of encryption by terrorist organizations is impacting your ability to detect and prevent future attacks, and how the proliferation of encryption alters the way you do business at the National Security Agency [NSA] and Cyber Command [CYBERCOM].

Admiral Rogers, you have frequently spoken with this committee about the so-called "dual hat" under which the Commander of Cyber Command also serves as the Director of the NSA. Last year, you told this committee, quote, "I will strongly recommend, to anyone who asks, that we remain in the 'dual-hat' relationship. This is simply the right thing to do for now, as the White House reiterated in late 2013." You stated that it might not be a permanent solution, but that it is a good solution, given where we are. You were asked again in our hearing earlier this year, and you reaffirmed the need to keep the two organizations tightly aligned.

That's why I'm troubled by recent reports that the Obama administration may be trying to prematurely break the dual-hat before President Obama leaves office. On Friday, it was reported that Secretary of Defense Ash Carter and Director of National Intelligence [DNI] James Clapper have backed a plan to separate Cyber Command and the NSA. Here we go again. Another major policy matter has apparently been decided, with no consultation whatsoever between the White House or the Department of Defense with this committee. I urged Secretary Carter to provide this committee and the Congress the details of this plan and his reasoning for support it. I will—hope he will explain what has changed since the last time the administration rejected this idea, in 2013.

While I'm sure the phrase "predecisional" is written somewhere in our witnesses' briefing papers, I would remind them that this committee does not take well to being stonewalled while their colleagues in the administration leak information to the press. Even if this decision has not been made, our witnesses should still be able to provide substantive analysis on the consequences of separating the dual-hat for our national security and for taxpayers.

Let me be very clear. I do not believe rushing to separate the dual-hat in the final months of an administration is appropriate, given the very serious challenges we face in cyberspace and the failure of this administration to develop an effective deterrence policy. Therefore, if a decision is prematurely made to separate NSA and Cyber Command, I will object to the confirmation of any individual nominated by the President to replace the Director of the National Security Agency if that person is not also nominated to be the Commander of Cyber Command.

This committee and this Chairman are tired of the way that Congress, in general, and this committee is treated by this administration. These issues present larger concerns about whether the Department is appropriately organized to manage the defensive and offensive requirements of the cyber mission. We know that the Department faces challenges in recruiting and retaining top cyber talent. We know that the Department's cumbersome acquisition system hinders technological advancement and has eroded our technological superiority. We know that the administration's failure to confront deficiencies in its cyber policy has undermined the Department's ability to effectively defend, deter, and respond to our adversaries in cyberspace. Both Russia and China have leveraged cyber to systematically pillage certain critical defense technologies, create uncertainty in our networks, and demonstrate capability. Make no mistake, they are the first movers in the cyber domain, and they have put us on the defensive. The administration has consistently failed to provide a meaningful response.

The latest media reporting, that Russia may try to undermine our electoral process, underscores this point. Russia is using cyber to undermine American national interest, and now it appears our democracy could be the next target. The administration's response to a mere warning from the Secretary of Defense—is that the best the United States can do? Despite this committee's numerous requests for a cyber deterrence framework, the administration has failed to present any meaningful strategy. Instead, it has evidently distracted itself with debates over the dual-hat. Instead of shaping

the limits of acceptable behavior in cyberspace, the administration, instead, has allowed Russia and China to write the playbook. As a result, this administration has left the United States vulnerable.

I look forward to hearing more about the cyber operations against ISIL and the challenges, opportunities, and constraints you are facing on the cyber front.

Senator Reed.

STATEMENT OF SENATOR JACK REED

Senator REED. Well, thank you very much, Mr. Chairman.

Let me join you in welcoming Secretary Lettre and Admiral Rogers back to the committee.

Thank you, gentlemen, and the men and women that you lead, for their service and your service.

This is a third committee hearing focused on the encryption issue, which underscores the importance of this issue and its impact on national security. The rapid growth of sophisticated end-to-end encryption applications and extremely secure physical access control to smartphones and computers has an adverse impact on law enforcement agencies at all level of government, and impairs the ability of the intelligence community and the Defense Department's Cyber Command to detect and counter cyber threats to the Nation. At the same time, this security technology helps to protect individuals, corporations, and the Government against cybercrime, espionage, terrorism, and aggression.

While Federal Bureau of Investigation [FBI] Director Comey has tirelessly stressed the danger of law enforcement going dark, respected national security experts, including General Michael Hayden, former Director of the Central Intelligence Agency [CIA] and NSA, Michael Chertoff, the former Under Secretary—or Secretary, rather, of Homeland Security, have advised against compelling industry to ensure that the Government can always get access to encrypted data. These experts argue that cyber vulnerabilities are the greatest threat to the public and national security. This debate underscores the complexity and difficulty of the issue that we all face and we all must deal with very quickly, because it is a growing—as the Chairman's testimony indicates, it's a growing threat to our national security and our law enforcement.

A major problem for law enforcement at this juncture is gaining access to data on devices that are physically in their control for foreign intelligence collection, where physical access is rarely, if ever, applicable, the challenges to overcome encryption of data in transit, or to gain remote access to devices when they are turned on and communicating. The latter set of problems is not qualitatively new. I will ask, when questioning, whether they're more manageable than these law enforcement issues.

In addition to encryption, another important area that I hope we're able to discuss today is the issue that the Chairman brought up. That's the future of Cyber Command. I understand the administration is deliberating on whether it is the proper time to elevate Cyber Command to a unified command, and if, and under what conditions, the administration should terminate the so-called "dual-hat" arrangement in which the Commander of Cyber Command serves also as the Director of the NSA. An additional issue, a dis-

cussion of whether the Director of NSA should be a civilian rather than a general officer. While I know that is likely difficult for our witnesses to discuss administrative deliberations in an open hearing, I will welcome any of your thoughts or considerations on these important issues.

Another area that I know is of interest to the committee, but, again, may be difficult to comment on publicly, is several revelations of hacking of major computer systems in this country by outside actors. Again, that is a very critical issue and one that we're very much involved and interested in.

Once again, gentlemen, thank you for your service, and thank you for your appearance here today.

Chairman MCCAIN. Now Secretary Lettre.

STATEMENT OF HONORABLE MARCELL J. LETTRE II, UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Mr. LETTRE. Chairman McCain, Ranking Member Reed, and members of the committee, thank you for inviting us to discuss the importance of strong encryption, trends on its use, and its impact on the Department of Defense.

With your permission, I have a written statement that is a little longer than my opening statement here, and I'd ask that it be made part of today's record.

In my brief opening statement, I would like to underscore three points:

First, the Department of Defense strongly seeks robust encryption standards and technology vital to protecting our warfighting capabilities and ensuring that key data systems remain secure and impenetrable to our adversaries today and well into the future. The Department's support for the use of strong encryption goes well beyond its obvious military value. For example, commercial encryption technology is not only essential to U.S. economic security and competitiveness, but the Department depends upon our commercial partners and contractors to help protect national security systems, research-and-development data related to our weapon systems, classified and sensitive information, and servicemembers' and Department civilians' personally identifiable information and health records.

Second, we are concerned about adversaries, particularly terrorist actors, using technology innovation, including ubiquitous encryption, to do harm to Americans. The cybersecurity challenges confronting the Department are compounded by the pace and scope of change, not only in the threat environment, but also in associated technologies. Our adversaries are constantly searching, looking, and adopting new and widely available encryption capabilities, with terrorist groups such as the Islamic State of Iraq in the Levant, ISIL, leveraging such technology to recruit, plan, and conduct operations. Our concern grows as some parts of the communication technology industry move towards encryption systems that providers themselves are incapable of un-encrypting, even when served with lawful government requests to do so for law enforcement or national security needs. This presents a unique policy challenge, one that requires that we carefully review how we manage the tradeoffs inherent in protecting our values, which include

individual privacy as well as our support for U.S. companies' ability to innovate and compete the global economy, and also protecting our citizens from those who mean to do us grave harm.

Third, the Department is working with other parts of the Government and the private sector to seek appropriate solutions on these issues now. We need to strengthen our partnership with the private sector, finding ways to protect our systems against our adversaries' cyberattacks and at the same time finding innovative and broadly acceptable ways to address nefarious actors' adoption of new technologies, including encryption, even while we must carefully avoid introducing any unintentional weaknesses in the protection of our security systems or hurting our global economic competitiveness.

Mr. Chairman, the Department is committed to the security and resiliency of our data and networks, and to defending the U.S. at home and abroad. An ongoing dialogue with Congress as well as other departments and agencies and the private sector is absolutely critical as we work together to confront and overcome the security challenges associated with encryption.

I appreciate the committee's interest in these issues, grateful for the dialogue, and I look forward to your questions.

[The prepared statement of Mr. Lettre follows:]

PREPARED STATEMENT BY THE HONORABLE MARCEL LETTRE

INTRODUCTION

Chairman McCain, Ranking Member Reed, and Members of the Committee, thank you for inviting us to discuss the importance of strong encryption, trends on its use, and its effects on the Department of Defense (DOD). It is an honor to appear before you today and we appreciate the opportunity to explain both the importance of encryption to secure data and to protect systems vital to our national defense, as well as the impact that the continuing adoption of strong encryption has on the execution of our national security missions. The use of strong encryption is a vital component to protect our warfighting capabilities and ensures our national security interests remain secure.

IMPORTANCE OF STRONG ENCRYPTION

The Department supports the use of strong encryption. Commercial encryption technology is vital to U.S. competitiveness and economic security and the Department depends upon secure data and strong encryption technology to carry out our national security mission. DOD depends upon our commercial-sector partners to help protect national security systems, research and development data related to our weapons systems, classified and sensitive information, servicemembers' personally identifiable information and health records, just to name a few examples. The National Security Agency (NSA), which is responsible for setting encryption standards within the Department of Defense, depends upon strong and voluntary commercial industry partnerships to protect these systems and to develop best practices on the implementation and integration of encryption.

If our adversaries are able to gain access to our networks, weapons systems, and other critical infrastructure, they could manipulate information, destroy data, and harm our national security systems. We must stay ahead of our adversaries' capabilities to ensure that our systems remain protected. Strong encryption remains a vital element to do so.

ENCRYPTION CHALLENGES

The threat landscape continues to change. The widespread availability of strong encryption has also allowed terrorist groups, such as the Islamic State of Iraq and the Levant (ISIL), to leverage such technology for its operations. ISIL uses the internet and mobile applications to securely communicate and recruit fighters, further incite violence, and inspire, plan, and conduct attacks against its enemies, including our forces. As terrorist groups become more sophisticated and techno-

logically savvy, encryption presents a challenge for the Department, especially NSA, to acquire needed intelligence if communications cannot be decrypted. This challenge will compound as industry moves towards implementation of encryption that they are incapable of unencrypting as they will no longer hold the decryption keys enabling them to provide access to the content of communications.

While the Department benefits from strong encryption, malicious actors use the accessibility of strong encryption and other technologies to thwart DOD efforts in a variety of areas. This presents a unique challenge for government, one that requires the nation to determine how to balance individual privacy, a fundamental tenet in our democracy, with the need to protect our citizens from those who would do harm. As we have seen with ISIL, terrorists are increasingly using strong encryption to hide the content of their communications. This challenges the ability of the Department to understand our adversaries' intent, terrorist networks, financing streams, tactics, attack planning and execution, in the United States and abroad.

ENCRYPTION WAY AHEAD

We need to strengthen our partnership with industry to find ways to protect against the national security threats to the United States. We will continue to work closely with our industry partners to find innovative ways to outmaneuver malicious actors' adoption of strong encryption, while ensuring that individual privacy interests are protected. I believe any steps we take as a government must be carefully considered to avoid introducing unintentional weaknesses in the protection of our commercial networks and national security systems. We should also be careful not to negatively affect our economic competitiveness as a world leader in technology, which could unintentionally drive technology innovation outside the United States.

CONCLUSION

The Department is committed to the security and resiliency of our data and networks and for defending the U.S. interests at home and abroad. Our relationship with Congress as well as other Departments, Agencies, and industry is absolutely critical as we work together to navigate the encryption challenge. I am grateful for the committee's interest in these issues, and I look forward to your questions.

Chairman MCCAIN. Admiral Rogers.

STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, COMMANDER, UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES

Admiral ROGERS. Chairman McCain, Ranking Member Reed, and members of the committee, thank you for the opportunity to appear before you today to discuss the current communications environment, including strong encryption and cyber challenges.

When we last met, on the 12th of July in a closed session, I outlined several of those challenges to the committee. Today, I look forward to further discussion so the American people are provided the greatest amount of information possible on these important topics. Of course, some aspects of what we do must remain classified to protect national security, so today I will limit my discussion to those in the public domain.

When I use the term "encryption," I'm referring to a means to protect data from any access except by those who are authorized to have it. Encryption is usually done by combining random data with the data you want to protect. The random data is generated by a mathematical algorithm and uses some secret information only, called a key, in the generation. Without the key, you can't undo the encryption.

NSA supports the use of encryption. It's fundamental to the protection of everyone's data as it travels across the global network. NSA, through its information assurance mission, for example, sets

the encryption standards within the Department of Defense. We understand encryption. We rely on it, ourselves, and set the standards for others in the U.S. Government to use it properly to protect national security systems. At the same time, we acknowledge encryption presents an ever-increasing challenge to the foreign intelligence mission of NSA. The easy availability of strong encryption by those who wish to harm our citizens, our government, and our allies is a threat to our national security. As you well know, the threat environment, both in cyberspace and in the physical world, is constantly evolving, and we must keep pace in order to provide policymakers and warfighters the foreign intelligence they need to help keep us safe.

Terrorists and other adversary tactics, techniques, and procedures continue to evolve. Those who would seek to harm us, whether they be terrorists or criminals, use the same internet, the same mobile communication devices, the same software and applications, and the same social media platforms that law-abiding citizens around the world use. The trend is clear. The adversaries continue to get better at protecting their communications, including through the use of strong encryption.

I want to take this opportunity to assure you and the American people that the NSA has not stood still in response to this changing threat environment. We are making investments in technologies and capabilities designed to help us address this challenge. Last year, we started a process to better help position ourselves to face these challenges.

It is premised in the idea that, as good as NSA is—as it is at foreign intelligence and its information assurance mission, the world will continue to change. The goal is, therefore, to change, as well, to ensure that we will be as effective tomorrow as we are today. The Nation counts on NSA to achieve insights into what is happening in the world around us, what should be of concern to our Nation's security, the safety and well-being of our citizens and of our friends and allies.

We have a challenge before us. We are watching sophisticated adversaries change their communication profiles in ways that enable them to hide information relating to their involvement in things such as criminal behavior, terrorist planning, malicious cyber intrusions, and even cyberattacks. Right now, technology enables them to communicate in a way that is increasingly problematic for NSA and others to acquire critical foreign intelligence needed to protect the Nation or for law enforcement individuals to defend our Nation from criminal activity.

The question then becomes, What's the best way to deal with this? Encryption is foundational to the future. The challenge becomes, given that premise, What is the best way for us ensure the protection of information, the privacy and civil liberties of our citizens, and the production of the foreign intelligence necessary to ensure those citizens' protection and safety? All three are incredibly important to us as a Nation.

You've also asked me to talk about cyber deterrence and U.S. Cyber Command's organizational structure. As I have said before, I do not believe that malicious cyber activity by adversaries can only be, or must be, deterred by cyber activity. Our Nation can

deter by imposing costs in and through other domains as well as using a whole-of-nation approach. Our instruments—all instruments of power should be considered when countering cyber threats, intrusions, or attacks.

With regard to our organizational structure, U.S. Cyber Command is well along in building our Cyber Mission Force, deploying teams to defend the vital networks that undergird DOD operations to support combatant commanders in their missions worldwide, and to bolster DOD's capacity and capabilities to defend the Nation against cyberattacks of significant consequence.

I, too, ask that my previously submitted written statement be made a part of the record.

I look forward to your questions, sir.

[The prepared statement of Admiral Rogers follows:]

PREPARED STATEMENT BY ADMIRAL MICHAEL S. ROGERS

Chairman McCain, Ranking Member Reed, and Members of the Committee, thank you for inviting me. It is a distinct honor and privilege to appear before you today. I appreciate this opportunity to speak to you about the current communications environment, including the wide availability of strong encryption, and its impact on the National Security Agency as we conduct our foreign intelligence and information assurance missions.When we last met on 12 July, I outlined several of these challenges to the Committee, and today I look forward to discussing those challenges so that the American people are provided the greatest amount of information possible on this topic.

When I use the term encryption, I am referring to a means to protect data from any access except by those who are intended or authorized to have it. Encryption is usually accomplished by combining random data with the data you want to protect. The random data is generated by mathematical algorithm and uses secret information—called a key—in the generation. Without the key, you cannot unlock the encryption, and access the data.

First and foremost, you should know that NSA supports the use of encryption. Encryption is fundamental to the protection of everyone's data as it travels across the global network. NSA, through its Information Assurance mission, sets the standards for the use of encryption within the Department of Defense. We understand encryption, rely on it ourselves, and set the standards for others in the government to use it properly to protect national security systems. At the same time, encryption presents an ever-increasing challenge to, our foreign intelligence mission. The easy availability of strong 1encryption by those who wish to harm our citizens, our government, and our allies is a threat to national security.

As you well know, the threat environment—both in cyberspace and in the physical world—is constantly evolving, and we must keep pace in order to provide our policy makers and war fighters the foreign intelligence they need to keep us safe. Terrorists' tactics, techniques, and procedures continue to evolve. Those who would seek to harm us use the same internet, the same mobile communications devices, and the same social media platforms that law-abiding citizens around the world use. The trend is clear, terrorists are becoming more savvy about protecting their communications—including through the use of strong encryption.

NSA has not stood still in response to this changing landscape. We are making investments in technologies and capabilities designed to help us address this challenge and last year, we started a process to better position NSA to face these challenges. It's premised on the idea—that as good as NSA is at its foreign intelligence and its information assurance missions, the world will continue to change. The goal is therefore to change as well in order to ensure we will be as effective tomorrow as we are today. The nation counts on NSA to generate insights into what is happening in the world around us, what should be of concern to our nation's security, the safety and well-being of our citizens, and of our friends and allies. We asked ourselves: how do we continue to generate the same level of information assurance or foreign intelligence or computer network defense insight given these changes? We see technology fundamentally changing—the proliferation of strong encryption across the internet and mobile devices is just one part of that change.

I told my team that I wanted us to think about what 2025 will look like and how we can better position NSA for that future. We call this effort NSA in the 21st Cen-

tury, or NSA21. As we look out to 2025, we see technology fundamentally changing in a variety of ways. Encryption tends to be getting a lot of attention at the moment, but the nature of technology's change is so much broader than that.It's encryption. It's the Internet of Things. It's the increased interconnectivity that is being built into every facet of our lives.

We have a challenge before us. We're watching sophisticated adversaries change their communication profiles in ways that enable them to hide information relating to their involvement in things such as criminal behavior, terrorist planning, malicious cyber intrusions, and even cyber attacks. Right now technology enables them to communicate in a way that is increasingly problematic for NSA to acquire critical foreign intelligence needed to protect the nation or for law enforcement officers to defend our nation from criminal activity.

The question then becomes, so what's the best way to deal with that? Encryption is foundational to the future. Anyone who thinks we are just going to walk away from that, I think, is totally unrealistic. The challenge becomes, given the premise that encryption is foundational to the future, what's the best way for us to ensure the protection of information, the privacy and civil liberties of our citizens, and the production of the foreign intelligence necessary to ensure their protection and safety?All three are incredibly important to us as a nation.

Thank you.I look forward to your questions.

Chairman MCCAIN. Thank you very much, Admiral. Is it still your professional military advice that maintaining the dual-hat at the—at this time is in our best national security interest?

Admiral ROGERS. Yes.

Chairman MCCAIN. General Dempsey stated that cyber is the one area we lack an advantage over our adversaries. Do you agree—still agree with that statement, Mr. Secretary?

Mr. LETTRE. I do agree that cyber—that the cyber threat is one of the greatest challenges we face.

Chairman MCCAIN. Admiral?

Admiral ROGERS. Yes.

Chairman MCCAIN. Russian activity reporting hacking on our electoral process, I find it interesting that one of the two States there seems to be evidence of it is the State of Arizona. What can you tell us about the Russian activity and reported hacking on our electoral process? Do you think this is acceptable?

Admiral Rogers?

Admiral ROGERS. Sir, as this is an ongoing investigation and a public, unclassified forum, I'm not going to be able to provide you specifics as to what our current assessment is. I will say this. This continues to be an issue of great focus, both for the foreign intelligence community, attempting to generate insights as to what foreign nations are doing in this area, as——

Chairman MCCAIN. This is the first time we've seen attempted interference in an—in elections in the United States of America, isn't it, Admiral?

Admiral ROGERS. Sir, we continue to see activity of concern. Again, I'm not going to characterize this activity "Is it a foreign nation-state, or not?"

Chairman MCCAIN. Mr. Secretary, you have anything to add to that?

Mr. LETTRE. Senator, I just would underscore that these are activities that the government is taking quite seriously. The FBI and the Department of Homeland Security [DHS] has an aggressive investigation underway, so the government can form its conclusion.

Chairman MCCAIN. Do we have a policy as to how to respond to this interference in elections in the United States of America? Do we have a policy as to what our actions be taken?

Mr. Secretary?

Mr. LETTRE. In this particular instance, Senator, the government is intending to rely on the results of the investigation being led by the Bureau to——

Chairman MCCAIN. I'm asking if——

Mr. LETTRE.—inform its policy decisions.

Chairman MCCAIN.—we have a policy, and the answer is no.

Admiral Rogers, there's a Wall Street Journal article yesterday, "New Tricks Make ISIS, Once Easily Tracked, a Sophisticated Opponent." Goes on and talks about how incredibly sophisticated some of their work was in preparation for these attacks—electronic silences; when they did communicate, called or sent text messages; location; cheap burner phones, et cetera. What are we—what would you think about this kind of activity, Admiral?

Admiral ROGERS. ISIL remains the most adaptive target I've ever worked in 35 years as an intelligence professional, sir.

Chairman MCCAIN. It was—is not a leap of the imagination to think that this kind of activity and planning further attacks on the United States is taking place as we speak?

Admiral ROGERS. Yes, sir.

Chairman MCCAIN. Admiral Rogers and Mr. Secretary, do you believe there's a legislative solution that can address some of these challenges we're talking about?

Mr. LETTRE. Senator, it—from my view, the legislative route is not something that we think is the best way to go, at this time. New legal and regulatory approaches are not as potentially productive as a robust dialogue seeking cooperation and collaboration with the private sector.

Chairman MCCAIN. I agree. Unless there is a policy about what the United States actions will be in the case of a threat, in the case of actual attack, in the case of other aspects of this challenge we're on, then you're going to see legislation. Right now, there is no policy. There is no policy that you can describe to me as to what we would do about an impending attack or what we would do about an attack. There's a vacuum there. If you don't act, then I guarantee you the Congress will act.

Admiral Rogers, it was recently reported that Twitter barred Data Miner, a company specializing in searching across millions of tweets to identify unfolding terrorist attacks and political unrest, from accessing its realtime stream of tweets because of its work for U.S. intelligence agencies. According to an article in the Wall Street Journal, this service gave the U.S. Intelligence Committee—community an alert about the Paris terrorist attacks shortly before they began to unfold last November. In March, the company says—first notified clients about the Brussels attacks ten minutes ahead. It also appears that Twitter will continue allowing information to be sold for use in the private sector, not just the government. Help me out, here.

Admiral ROGERS. I wish I could, Senator. I am perplexed by their approach in this particular instance.

Chairman MCCAIN. We have a situation where—excuse me—we have a situation where we have the ability to detect terror attacks using organizations' such as Data Miner, and yet, in order for us to anticipate these attacks, we have to have certain information.

Twitter is refusing to allow them to have information which literally could prevent attacks on the United States of America? Is that the situation here, Admiral?

Admiral ROGERS. Yes, sir. At the same time, still willing to provide that information to others for business purposes.

Chairman MCCAIN. For sale.

Admiral ROGERS. For sale, for revenue.

Chairman MCCAIN. What do you think we ought to do about people like that, besides expose—besides exposing them for what they are?

Admiral ROGERS. Clearly, I wish I had better understanding—and perhaps there's insights that I'm just not aware of—I wish I had better understanding as to the rationale that leads someone to believe that that is the right course of action. I'm just the first to acknowledge, I don't understand it.

Chairman MCCAIN. Shame on them.

Senator Reed.

Senator REED. Thank you very much, Mr. Chairman.

One of the issues—and it's the last line of questioning, and it's highlighted quite a bit—is that what used to be the domain of nation-states—sophisticated research, development, application of products—are now done commercially all across the globe. I mean, some of these encryption devices were just adapted by ISIL, they weren't developed by ISIL, but they've been very effective. We're in a race not just against another nation-state, we're in a race against technical innovation that is widespread and is relatively inexpensive, in terms of the commitment you have to make to develop a product. Is that a fair assessment, Admiral Rogers?

Admiral ROGERS. Yes, sir. I often use the phrase, "Cyber is the great equalizer." It doesn't take billions of dollars of investment, it doesn't take tens of thousands of dedicated individuals, and it's—uses a set of capabilities that are readily available globally to a host of actors.

Senator REED. I think it's incumbent upon us to approach it not as we've done in the past, you know, a nation-state, to countering their technology, but with a much more, you know, innovative approach.

Let me ask both you and the Secretary, What is this new innovative approach to counter this new decentralized, disaggregated, relatively inexpensive ability to upset our very expensive and elaborate systems, both platforms and intelligence systems?

Mr. LETTRE. Senator, I'd just make a couple of broad points on this.

The most important thing we need to do in the Department of Defense is reach out to any and all partners that can help us find solutions. For example, the Department's senior leadership has invested heavily in conversations with leadership across the U.S. technology sector to really seek a dialogue about how we can come up with innovative solutions to address the dynamics you've raised, which include a quick and agile set of adversaries being able to adapt to new technologies, themselves, and leveraging those technologies to conduct global messaging that advances their interests. We've got to find a way to outpace that. We believe that we can

do so by tapping into the best ingenuity that the American private sector has to offer.

Senator REED. Admiral?

Admiral ROGERS. The other thing we're trying to do, at an operational level, in addition to the power of partnerships, which I agree with Marcell is very important for us—the argument I'm trying to make on both the NSA and the Cyber Command side is, "Guys, we're dealing with a whole new ecosystem out there, and we've got to bore into this ecosystem and look at it in just that way. Don't focus on just one particular application as used by one particular target. Think more broadly about the host of actors that are out there, about how that"—and I apologize, I can't get onto specifics in an open forum, but looking at it more deeply, not just the one particular app, if you will, used by one particular target, that if we look at this more as an ecosystem, we will find vulnerabilities that we can access to generate the insights that the Nation and our allies is counting on.

Senator REED. I think, fundamental to your approach—and again, it touches on the issues raised by the Chairman—is that if these large technological players or, you know, civilian potential partners refuse to cooperate, then that is very—could be detrimental in our security. We have to find a way either to convince them or otherwise get them to cooperate, because I—my sense is, without it, that we will not be able to deal with this issue. Is that fair?

Admiral Rogers?

Admiral ROGERS. It is, from my perspective. Partnerships is going to be incredibly foundational to the future, here.

Senator REED. Just a final point. Raise it. You might comment quickly. That is, you know, there's been some discussion about having sort of a key to these encryption so that—you know, the proverbial backdoor—so that government could get in, et cetera. Opponents to that approach suggest that that—not only government could get in, but other bad actors could get in. Is that a solution that causes more problems, or is that a real solution?

Mr. LETTRE. Senator, from a policy perspective, we're in favor of strong encryption. We benefit from it, ourselves. Anything that looks like a backdoor is not something we would like to pursue. The important thing, I think, is, on a case-by-case basis, for institutions like the Department of Defense and the Federal Bureau of Investigation and other key stakeholders, to have a really rich dialogue, case by case, with key industry players to see what kinds of solutions can be brought to bear, given the imperative to also balance privacy and civil liberties for our public, as well as to be able to ensure the competitiveness of our economic players.

Senator REED. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. If I—Senator Rounds will indulge me one second.

Admiral, I just want to go back to this election in Arizona. Is it possible that Russians could somehow harm the electoral process in my home State of Arizona?

Admiral ROGERS. Senator, let me plead ignorance on the specifics of the electoral system in the State of Arizona.

Chairman MCCAIN. Or is it—is there a possible scenario where they could disrupt the voting results in the upcoming election?

Admiral ROGERS. I think there are scenarios where you can see capability applied in particular areas. Again, it's not—I don't have strong fundamental knowledge across the breadth of the 50 States, since elections are run on a——

Chairman MCCAIN. Yeah.

Admiral ROGERS.—State basis. One advantage I do see, from a defensive standpoint, is that the structure is so disparate, with some elements being very—still very manually focused, others being more electronically and interconnected—because it's not just one nationwide, single, integrated structure, that tends to help us, I think, defensively, here.

Chairman MCCAIN. It is a concern.

Admiral ROGERS. Oh, yes, sir.

Chairman MCCAIN. Senator Rounds. Thank you, Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman. Thank you, to you and the Ranking Member, for putting this subject before us today.

I have a number of questions concerning how we respond to a cyberattack on civilian infrastructure. I'm just curious. I know that the Chairman has already raised the question of a policy, but I'd like to go a little bit deeper. What I'm really curious about is, what is the role of the Department of Defense with regard to an attack on civilian critical infrastructure? Is there a preemptive responsibility that the Department of Defense has to protect civilian infrastructure in a cyberattack, similar to what happens with a kinetic attack?

Mr. LETTRE. Senator, from a policy perspective at DOD, we have three main missions. One is to defend the Defense Department and its networks. The second is to support our commanders in providing military options in support of their plans and operations that relate to cyber. The third is, when called upon by the President and the national command leadership, to support broader efforts that might be brought to bear in the case of an attack on U.S. critical infrastructure.

Senator ROUNDS. Has that occurred? Has that request occurred yet?

Mr. LETTRE. Well, it—the request typically would come in, in a specific instance of an attack.

Senator ROUNDS. In the case of an attack on a civilian infrastructure, how long would it take from the time that the attack is initiated until a time that the damage is done? Milliseconds?

Mr. LETTRE. It really depends on the circumstances of the attack, but it can be pretty quick, in the case of a cyberattack, yes.

Senator ROUNDS. How in the world would we expect the President of the United States, even if it's not at 3:00 o'clock in the morning, to respond in time to give you permission to protect critical civilian infrastructure if you already don't have a plan in place? Or do you have a plan in place?

Mr. LETTRE. Right. There—at the policy level, there has been a multiyear effort to develop that overall framework for how to respond to attacks.

Senator ROUNDS. No——

Mr. LETTRE. Then operationally——

Senator ROUNDS.—either you've got one——

Mr. LETTRE.—there are systems, as well.

Senator ROUNDS.—in place today or you do not. Do you have a plan in place today to respond to an attack on critical civilian infrastructure?

Mr. LETTRE. I believe we do have a plan in place, Senator. In July, for example, the President approved something called the Presidential Policy Directive on Cyberincident Coordination, PPD–41, which lays out a framework for an interagency effort to respond to attacks on our critical infrastructure from a cyber perspective.

Senator ROUNDS. You would not have to respond——

Mr. LETTRE. In addition——

Senator ROUNDS.—you would not have to wait for a presidential directive to protect critical infrastructure today.

Mr. LETTRE. That's right. Now, there are a whole host of operational implications that need to follow from that. Each department and agency has worked through what capabilities it brings to bear and how quickly, operationally, those can be applied. In the case of the Department of Defense, obviously, we look very quickly to the capabilities of U.S. Cyber Command.

Senator ROUNDS. Admiral Rogers, today——

Admiral ROGERS. Sir.

Senator ROUNDS.—can we protect critical infrastructure if it is under a cyberattack?

Admiral ROGERS. Do I have the capability to protect aspects of critical U.S. infrastructure? Yes, sir.

Senator ROUNDS. Thank you.

Let me go back. I—you know, in the news, you've all heard, and we've all heard, about the discussions regarding Secretary Clinton's use of the email systems and so forth. One of the things that concerns me—and I'd just like you to maybe put this in perspective for me if you could—one of the ways in which we lose information or in which data that is private, confidential, classified is released, is not necessarily through unfriendly actors getting a hold of or breaking into our encrypted information, but simply human error and individuals within government who have access to classified or confidential information, or information which is classified at a higher category than that. Could you talk to us a little bit about what the responsibility is and whose responsibility it is to actually train or to give information to individuals who are either elected, appointed, or hired by the government to make sure that they understand the differences between the categories, between whether a "C" means that it's in alphabetical order or it is confidential or any classified setting? Whose responsibility is it within the governmental layout, the structure today, to see that that information is appropriately disseminated and that instructions and remedial instructions are provided if there is a break? Where does that fit?

Mr. LETTRE. Senator, the questions around cyber hygiene, essentially, and how to properly protect yourself against IT intrusions and so forth is one set of policies and practices that typically the CIOs and associated IT security managers have responsibility for educating government employees at all levels. There are also aspects around the handling of classified information that flow from

security policies and procedures, and those are typically handled by departments' security subject-matter experts.

Senator ROUNDS. Department by department?

Mr. LETTRE. Typically so, yes, sir.

Senator ROUNDS. Who oversees that information—or the delivery of that information?

Mr. LETTRE. Well, the——

Senator ROUNDS. Your agency?

Mr. LETTRE. The—in the case of the Department of Defense [DOD], for DOD employees, my office oversees the setting of security policy standards.

Senator ROUNDS. Mr. Chairman, thank you.

Chairman MCCAIN. Senator Nelson.

Senator NELSON. Admiral, I have often thought of our ability to protect ourselves in cyber as that we are really almost like the standoff in the nuclear, assured mutual destruction. It gets more complicated with this, because we have nonstate actors. Could you give us an example, in this open setting—and, if required, then in a classified setting—of where we have been attacked and we showed them that the return hit is going to be so hard that it deters them from hitting in the future?

Admiral ROGERS. Again, I can't get any details in an open forum, but I would suggest the response to the Sony hack by the North Koreans in November of 2014 is an example of that.

Senator NELSON. Is that in the public domain—that example?

Admiral ROGERS. In the sense that we publicly acknowledged both the event, we publicly acknowledged who did it, and we publicly discussed the steps we were going to take in response to it, and we also highlighted at the time, "If this activity continues, we are prepared to do more at the time and place of our choosing."

Senator NELSON. The specifics of that, will that have to be in a classified setting?

Admiral ROGERS. No, in the sense that, in this case, we chose to use the economic lever, it goes to one of the comments I made in my opening statement. One of the things I'm always recommending—I realize I just work the operational piece of much of this—but, I always encourage people, "Think more broadly than cyber. When thinking deterrence, think more broadly than cyber." Just because an entity, nation-state, group, individual comes at us in cyber, that doesn't mean that our response has to automatically fall back on, "Well, we have to respond in kind. We have to go back from a cyber perspective." I've tried to make the argument, as have others, we need to play to all of the strengths of our Nation. In the Sony case, for example, we collectively, from a policy perspective, made a choice to play to the strength of the economic piece for the United States.

Senator NELSON. Right. I think that's smart. You've got a menu of things.

Admiral ROGERS. Sir.

Senator NELSON. When you get right down to tit-for-tat, we could absolutely, with our attacks, shut down a number of things.

Admiral ROGERS. We could cause significant challenges to an opponent. I'm not going to get into specifics, but yes.

Senator NELSON. Right. Do—with state actors, do we see that that is actually creating a mutually assured destruction?

Admiral ROGERS. I would argue, not yet. Because remember, a part of deterrence is both—some aspects to deterrence—convincing someone that the benefit that they will gain doesn't justify the cost, convincing the actor that they just won't succeed, or convincing the actor that, "Even if you were to do this, and even if you were to succeed, what we'll bring back against you in response to this just doesn't merit you doing this. You really ought to think hard and fast before you really do this." I have said this multiple times publicly before. The challenge we have right now is, I think, for a variety of reasons, some—not all—some actors have not yet come to the conclusion that there's a significant price to pay for some pretty aggressive actions on their part in the cyber arena.

Senator NELSON. Well, I'd like to follow with you, in a classified setting——

Admiral ROGERS. Sir.

Senator NELSON.—how we might respond to some of those actors.

Admiral ROGERS. Sir.

Senator NELSON. In the private sector, do we have the cooperation that we need to tackle these encryption challenges?

Admiral ROGERS. At an operational level, my observation—because this is much bigger than just Cyber Command or NSA—my answer would be no, in the sense that—my sense, as I look at this problem set, I see multiple parties spending a lot of time talking about what they can't do or what can't be done. I wish we spent more time thinking about, Well, what could we do, what is in the realm of other possible? Even as I acknowledge I think there's multiple parts to this conversation. What can we do is not necessarily the same thing as what should we do. Those are two very important parts of this conversations that I think we need to have.

Senator NELSON. The encryption thing does trouble all of us.

Admiral ROGERS. Sir.

Senator NELSON. Aside from encryption, what other technology trends are shaping the way that the Department does business?

Admiral ROGERS. It—from a cyber perspective?

Senator NELSON. Yes.

Admiral ROGERS. We're very much interested in artificial intelligence, machine learning. How can we do cyber at scale, at speed? Because if we're just going to make this a largely human capital approach to doing business, that is a losing strategy. It will be both incredibly resource-intensive, and it will be very slow. I'd say that is a big area of focus for us. In addition, we're constantly reaching out—Defense Innovation Unit Experimental [DIUX], the capability that's been created out in Silicon Valley as well as Boston, U.S. Cyber Command has a separate but related—that teams with DIUX to try to harness partnerships in the private sector.

Overall, I'd say good. As the Chairman highlighted, every once in a while, you just run into a situation where you go, "Can't we just step back, sit down, and talk to each other rather than, you know, these arbitrary, 'Hey, you can't do this, you can't do that, we won't do this, we won't do that'?" Even as I acknowledge there are different perspectives out there, I have no issue with that at all. I certainly understand that.

Senator NELSON. Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Lee.

Senator LEE. Thank you, Mr. Chairman.

Thanks, to both of you, for being here. I also appreciate your commitment to protecting the rights that we hold dear as Americans, and our security.

This issue of encryption cuts right to the heart of a lot of things. It cuts right to the heart of the nature of the relationship between the American people and their national government, and to the heart of a number of features in the Constitution, including responsibilities of the Federal Government to safeguard the people and also to safeguard their rights.

I believe it's an issue that Congress and the executive branch have to approach with a great deal of prudence, recognizing that we can't view it exclusively either as a national security issue, on the one hand, or as a privacy issue, on the other hand. We have to view it holistically, understanding that we've got to find a resolution to this that respects all the interests at stake.

Admiral Rogers, I'd like to start with you. On August 17th, the Washington Post reported that a cache of commercial software flaws that had been gathered by NSA officials was mysteriously released, causing concerns both for government security and also for the security and the integrity of those companies who I believe had not been notified by the NSA of the flaws discovered in their systems. Can you walk through this process with us that the NSA uses to determine——

Admiral ROGERS. Vulnerability?

Senator LEE. Yeah. Well, to determine when, whether, to what extent you should notify a private company of a security vulnerability that you've discovered, and whether NSA will continue to withhold such information from those companies when you're holding those and there are some clear concerns about the security of your own systems.

Admiral ROGERS. There's a vulnerability evaluation process, interagency, that was started in 2014, that we continue to be a part of, whereas NSA and other entities, not just us, become aware of, you know, zero-day vulnerability, so to speak, those vulnerabilities that we don't think are—others are aware that haven't been patched or addressed, that we raise those through an interagency process, where we assess what's the impact of disclosing or not disclosing. I have said publicly before, I think, over the last few years, overall—I think our overall disclosure rate has been 93 percent or so of the total number of vulnerabilities using this process since 2014. We continue to use that process.

Senator LEE. Okay. Okay. You do that on a case-by-case basis——

Admiral ROGERS. Yes, sir.

Senator LEE.—depending on the totality of the circumstances.

Has there been an instance in which a U.S. company has suffered a security breach because of a cyber vulnerability that you were aware of that you—that NSA had previously identified but——

Admiral ROGERS. I can't say totality of knowledge, sir. I don't know totality. I apologize.

Senator LEE. Okay. No, it's understandable.

On Sunday, just this past Sunday, the Wall Street Journal published a report on the methods of ISIS, the methods that ISIS is using, in which there were some experts who concluded that low-tech communications, including things like face-to-face conversations, handwritten notes, and sometimes the use of burner phones, have proven to be just as much of a problem for Western intelligence officials as the use of high-end encryption by our adversaries.

Mr. Secretary, I was wondering if I could get your sense on this. Are the defense and intelligence communities investing enough into human intelligence and other activities to address low-tech terror methods, like those leading up to the Paris attacks? If we continue, I—a related question to that is, If we continue focusing on combating highly sophisticated encryption technology, do we expect to see a corresponding shift into these lower-tech alternatives?

Mr. LETTRE. Senator, you're—you've put your finger on a really important point, which is the need for a really diverse set of intelligence collection capabilities and disciplines. Capabilities that go after the high end, using the best of our technology available, but also capabilities that draw upon individual case officers, area expertise, language expertise, and presence on the ground in a lot of places around the world, where we can, in a very granular way, pick up what's going on and identify threat actors who, as you noted, may be using relatively unsophisticated mechanisms for planning and plotting attacks against the U.S. Homeland and our allies. With regard to the aspect of your question around human intelligence, we have been making some investments, over the last several years, to continue to improve the effectiveness and capacity of defense-related human intelligence, working closely with CIA. I think that that is a very important set of investments to be making.

Admiral ROGERS. Senator, could I add one comment?

Senator LEE. Sure.

Admiral ROGERS. That would be okay?

I think what that article highlights is the fact that we are watching ISIL use a multi-tiered strategy for how they convey information and insight that runs the entire gamut. I think, for us, as intelligence professionals, we've got to come up with a strategy and a set of capabilities that are capable of working that spectrum. It can't be we just spend all our money focused on one thing. I don't think that's a winning strategy for us, if that makes sense.

Senator LEE. Understood.

I've got a couple of other questions, but my time's expired, so I'll submit those in writing.

Thank you very much.

Chairman MCCAIN. Senator Heinrich.

Senator HEINRICH. Thank you, Mr. Chair.

Admiral Rogers, I want to continue along that line of questioning. Recently there was a worldwide survey, actually, of encryption products, looked at 865 hardware and software commercial encryption products that are available worldwide. About a third of those were developed in the U.S.; two-thirds were developed overseas. You know, it begs the question, If Congress were to

act on this issue, if Congress were to compel some sort of built-in backdoor to those kinds of products, would that in any way effectively limit access to strong encryption projects to our enemies, to foreign terrorist groups? So long as they're widely available on the Internet?

Admiral ROGERS. I think, clearly, any structure, any approach that we come up with here with respect to encryption has to recognize that there is an international dimension to this, that encryption doesn't recognize these arbitrary boundaries on the globe that we have drawn, in the form of borders of nation-states. I don't know what the answer is, but I certainly acknowledge we have to think more broadly than just one particular market, so to speak.

Senator HEINRICH. Given how easy it is to just download an app onto your smartphone to do end-to-end encryption of texting and other communications, does it—and getting to, really, Senator Lee's question—does it beg the question of whether or not we've become overly reliant on signals intelligence, generally? Are we investing enough in human intelligence?

Admiral ROGERS. I'll leave that up to the Under Secretary. I'm a——

Senator HEINRICH. I know it's dangerous question for someone in your position, but——

Secretary?

Mr. LETTRE. Senator, the short answer is, we do need to be investing in a range of capabilities, including the human intelligence capabilities. As to the point about individuals being able to download an app onto their mobile phones and smartphones that can avoid law enforcement or national security coverage, it really just underscores the imperative for a really rich and diverse set of conversations to be going on between government and all players across the technology sector. Each company has a different business model, which may or may not implement end-to-end encryption in a ubiquitous way, and we need to be looking for solutions on a case-by-case basis that allow us to preserve our values, including the ability to conduct law enforcement and national security protective operations in service of the Nation.

Senator HEINRICH. You know, one of the issues that was raised earlier is this idea of identifying vulnerabilities that may exist in software, in operating systems, in hardware. Obviously, when there are those vulnerabilities, it means that people who work for the U.S. Government, as well as private citizens, have data potentially exposed to nefarious actors. Has the administration ever considered some sort of reward structure, incentive structure for those sorts of vulnerabilities to be identified and, therefore, identified to companies so that they can plug those holes as they come up?

Admiral ROGERS. I can't speak for the administration as a whole, but we have done this twice now within the Department of Defense, you could argue, in the Bug Bounty Program, where we specifically have tried to incentivize the discovery and sharing of vulnerabilities, both to help the Department as well as to help the commercial sector in trying to address them. That's something that we've been doing.

Senator HEINRICH. Have you found that to be a—an effective strategy?

Admiral ROGERS. Yes, sir. In fact, you'll see us—in the coming months, we're looking at the next iteration of the program, as well. This is something we want to continue.

Senator HEINRICH. Do you think that's something we should be looking at as a more whole-of-government approach, as well?

Admiral ROGERS. I would only say, our experience has been a positive one, and I would fully expect that it would turn to be positive for others. The scale is——

Senator HEINRICH. I know with my conversations with the technology sector, that's something that's come up——

Admiral ROGERS. Right.

Senator HEINRICH.—consistently over time.

Thank you both.

Chairman MCCAIN. Senator Sullivan.

Senator SULLIVAN. Thank you, Mr. Chairman.

Thank you, gentlemen, for the testimony today.

Admiral Rogers, I just want to get—and I know you've been talking about this in a more broad sense, but what do you see as the three top threats that U.S. Cyber Command or the NSA have to plan or defend against? Top three. It can be a country or it can be an issue. When you're going to bed at night, what are the top three that you're——

Admiral ROGERS. Broadly, as I look out, number one is just the day-to-day defense of the DODIN. I look at DOD. We are a massive Department with a global laydown and a network infrastructure that was built in a different time and a different place, in which redundancy, resiliency, and defensibility were not core design characteristics. My challenge at the Cyber Command side is, I've got to defend an imperfect infrastructure and give us the time to make the investments to build something better. That's challenge number one. I'm always thinking to myself, what are the vulnerabilities out there that I don't recognize yet that someone's exploiting?

Number two would probably be—I worry about—most penetrations in networks to date have largely been about extracting information—extracting, pulling the data—whether it's to generate intelligence insights, whether it's to generate battlefield insights, whether it's to potentially attempt to manipulate outcomes. What happens when it's no longer just about data extraction, but it's about data manipulation, and now data integrity becomes called into question? As a military commander, if I can't believe the tactical picture that I am seeing, that I'm using to make decisions, that are designed to drive down the risk and help me achieve the mission, if what I'm seeing is a false representation and, in fact, the choices I'm making are increasing the risk and, in fact, are not having positive outcomes—data integrity, data manipulation really concerns me. That's a whole different kettle of fish.

Then the third one, probably, What happens when nonstate actors decide that the Internet is not just a forum to coordinate, to raise money, to spread ideology, but instead offers the opportunity to act as a weapon system, to employ capability on a global scale?

Senator SULLIVAN. Let me ask about that last one, because I think one of the things that we continually hear, in terms of our

cyber strategy and how it—and how the—this domain differs in so many other domains—is that the attacks, when they occur on us, seem to come, in some cases, without much cost. We're getting hit from all different angles, and we're not sure where or how, and you can't do a symmetrical smackdown, maybe. How do we—how do we raise the costs for adversaries who are attacking us in this domain? Or how do we signal that we're going to do it? Obviously, a lot of it—if we're signaling, we have to have credibility. How do we raise the cost? Do you think we do need to raise the cost? Do you think, in this domain, that our adversaries or potential adversaries think that they can take action and kind of get away with it because we're not going to respond? Do we need to be more aggressive in signaling how we're going to respond, and then respond?

Admiral ROGERS. I think we need to show adversary we have capability, we have intent, and we have the will to employ it, within a legal framework——

Senator SULLIVAN. Have we done that, though, much?

Admiral ROGERS. We have—as I've said, we've done it. The Sony piece, I would argue. You could also argue, in the areas of hostilities—Syria, Iraq, Afghanistan—we're doing some good things every day that clearly I think the opponent understands that we're applying this capability against them. We've publicly acknowledged that we are doing that. I think, in part, that idea of publicly acknowledging the fact that we were using cyber as a capability to counter ISIL was not just to signal ISIL, but was also to make sure others are aware that the Department of Defense is investing in these capabilities, we are prepared to employ them, within a legal, lawful framework.

Senator SULLIVAN. Do you think we're sending that signal to state actors in the cyberspace?

Admiral ROGERS. I certainly hope so, sir.

Senator SULLIVAN. Well, do you think we are? I don't know what——

Admiral ROGERS. I think it——

Senator SULLIVAN. You're the—you're in charge, right? "Hope" makes me a little worry. What you think——

Admiral ROGERS. It varies by the actor. Honestly. It varies by the actor.

Senator SULLIVAN. Do the Iranians fear that we could retaliate against them if they take some kind of cyber action?

Admiral ROGERS. Yes. My sense is, the Iranians have a sense for a capability. I apologize, I can't get into a lot of specifics, but my sense is, they have awareness of capability, and they've seen us use it.

Senator SULLIVAN. Let me ask this one final question. It seems to me, kind of longer term, one of the biggest strategic advantages we have in this domain is our youth and their capabilities, which far exceed, probably, everybody in this room, given how smart they are in this space and how they've just naturally grown up with it. What are we doing to make sure to try to recruit younger Americans to, you know, be on the right side of the issue, to come serve their country in a really critical area, where they, in many ways, have unique skillsets that a lot of us—no offense to my colleagues around the dais here—that a lot of us don't have?

Admiral ROGERS. Yes, sir. On the NSA side, I'll just highlight a couple of examples. We have a conscious effort that we've been doing for several years now. We do high school and junior high school cyber camps that we partner with a variety of institutions across the United States. We have cyber acquisition—or cyber academic excellence and academic research excellence relationships with over 200 universities on the NSA side across the United States, because we realize much of the workforce that we're looking to gain in the future is going to come from these pools. There's something to be gain, we believe, by interacting early with them, and, more broadly, for the Nation as a whole, helping to encourage the acquisition of these skills, this knowledge, in a way that just wasn't necessarily the case in the past.

Senator SULLIVAN. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

Thank both of you all for being here.

Admiral ROGERS. Sir.

Senator MANCHIN. Along the line of questioning there, for those of us who grew up in the not-Internet Age, if you look around at some of us here in the audience and some of us on this—and now all this coming to fruition, it's quite confusing, quite troubling, quite concerning. With all that being said, you know, we have concern over our food supply, our energy supply. The average person in America right now is concerned over, whether they have children or grandchildren, cyber bullying, everything that goes on with the Internet. We see the rise of terrorist—the great equalizer is the Internet for them. They don't have an air force, they don't have a navy. They have nothing more than the will to do us harm or wreak havoc around the world.

With all that being—going on, the question I would like to ask best is, In a perfect world, without the politics involved, not being—trying—being politically correct, what can we, as Senators sitting on this committee or in this body or in Congress, 535 of us, concentrate and do to allow you to streamline this to make this work? It looks to me like you're going to take a covey of volunteers around the country that are smart and bright, to recruit them, but also, if people are out there hacking us continuously, are they able to intercede? Are they able to see what's going on? Are they able to report—is there some way of communication that the average person say, "Listen, I've seen some activity going on here that I think is going to be detrimental to us, think you ought to know about." You all have a—an agency—I mean, a way that you can collect this information? What can we do to help to streamline this, to correct this, so it doesn't get so convoluted that something falls through the cracks?

Whoever wants to take that one, you can——

Mr. LETTRE. Senator, I'll take a first crack at it. Really, the most important thing, I think, that we can all do—and this committee and you all, as members, are incredibly powerfully well suited and seated to be able to do this—is to have that dialogue, catalyze that dialogue with the public, with civic leaders, with industry leaders, about the shared nature of this challenge, both the cybersecurity

challenge and the hacking that we all face across—from the individual to companies and governments, and the acute threat from—ongoing threat from terrorism, and the need to put our best foot forward, in terms of countering violent extremist messaging, countering their ability to recruit and persuade over the Internet. That——

Senator MANCHIN. I think——

Mr. LETTRE.—that dialogue with leaders to really impress upon corporate and civic leaders the need to have—view that as a shared problem and to really look for solutions with us.

Senator MANCHIN. Well, the question I'm asking, I think, to both of you all, is that—I mean, if you're looking at us as a—everybody says lack of money, it's always a money situation, to a certain extent, or is it a lack of, basically, siloing to where everyone's protecting their own territory? Is there a way that we can break through, that, if you're going to be that agency, there has to be one gathering point and, basically, one dispensing point. I'm understanding that some of our agencies aren't talking to each other. We have the situation to where we don't have the private sector cooperating—San Bernardino, Apple, and all that, that comes to mind. This can't happen. If that's the great equalizer, and we have people that have nothing else more than the will to do us harm, we have to have the will to protect greater than the will to do harm.

Admiral, I'm looking for just a way to help.

Admiral ROGERS. Senator, I don't disagree with many of the statements you're making. This is my takeaway, having done this for a while now. Using the same structures and the same processes and expecting different outcomes probably is not going to get us——

Senator MANCHIN. We understand that definition.

Admiral ROGERS.—where we want to be. I think the challenge, particularly as we're looking in the future, is, can we take the opportunity to step back and ask ourselves, "Hey, what do we need to be doing differently?"

The other thing, I think, particular as Senators, as among the leaders of our Nation, these are serious, hard issues, with a wide variety of perspectives, and we have got to get beyond this simplistic vilification of each other to roll up our sleeves and figure out, How are we going to make this work? Realizing that there's multiple perspectives and a lot of different aspects of this that have to come to the fore.

Senator MANCHIN. You know, I tell—I speak to children and—much as I possibly can. I would—and I tell them, I says, I don't think—nowhere in the world is there a military might that can challenge us. We have the greatest military in the world. The economy—our economy is greater than anyone in the world, almost double the closest—of China. I'm not worried about a military or an economic takeover of the United States of America. I worry every day about the cyber—breaking down the cybersecurity, how they hack and whack at us and, basically, come at us different ways. If we're not defending that, if we're not giving you the tools, and if we're playing politics, being Democrat and Republican and who's politically correct—this is not a time to do that.

I think there's a group of us here that would love to step out and say, "Okay, how do we streamline this? How do we make sure that someone says, 'We do this, or we don't do this, or we go in this direction'?" That's what we're looking for. Hopefully you know that we're here to help there.

Admiral ROGERS. Yes, sir.

Senator MANCHIN. Thank you.

Chairman MCCAIN. Senator Shaheen.

Senator SHAHEEN. Thank you, Mr. Chairman.

Thank you both for being here today.

I want to follow up a little bit on Senator Manchin's question, which was really referred back, I think, to Senator McCain and the Twitter example that you used earlier.

How do we get some of those private-sector companies to recognize that this a shared challenge and that we've got to work together? Do we need more legislation to address that? This is really a policy question for you, Secretary. Is it that, or is it meeting with folks? What do you think we need?

Mr. LETTRE. Senator, our view, at this point in the dialogue and debate, is that legislation that forced or required a regulatory solution is not preferred, at this point. What we have found is that, on a case-by-case basis, when leaders from the executive branch have been able to have a very effective, quiet dialogue with leaders in industry, that the nature of the conversation starts to shift in a couple of ways. One is, you know, industry and government, for decades, have worked together very proudly on projects that protect the Nation. Reminding ourselves of that rich history, I think, starts to put the conversation into a dialogue around solutions rather than being at odds with each other in an antagonistic way. If, on the government side, we're able to communicate the problems we're trying to solve and ask for industry's best expertise and wisdom about the solutions that might be brought to bear that we haven't even thought about yet, often we find that we are able to come up with solutions that meet our law enforcement and national security needs.

The second thing that I think is——

Senator SHAHEEN. Well, let me just——

Mr. LETTRE.—that we——

Senator SHAHEEN.—I'm sorry to interrupt, but has that worked with Twitter, in terms of the willingness of Twitter to allow us to scrub some of the information that they have?

Mr. LETTRE. As was mentioned earlier, to the best of my knowledge, Twitter's position hasn't changed on its level of cooperation with the U.S. intelligence community, so far.

Senator SHAHEEN. We were not very successful with Apple, either. Is that correct?

Mr. LETTRE. That's right, yeah.

Senator SHAHEEN. There are limits. Certainly, there are limits to that kind of a strategy. I appreciate what you're saying. I mean, I would—I have a—always rather try and sit down and resolve the situation rather than pass legislation, but right now we've had mixed reviews of the opportunity to work collaboratively with the private sector to address this issue.

Mr. LETTRE. Yeah, that's absolutely fair to say. Now, the industry and the private sector is very diverse. Businesses——

Senator SHAHEEN. Sure.

Mr. LETTRE.—have different business models, which leave them in different positions, as far as their ability or willingness to work closely with government on working our way through some of these law enforcement questions. It—a case-by-case approach, I think, is what is absolutely needed. As you pointed out, we are not successful in every case.

Senator SHAHEEN. I had the opportunity, earlier this year, to visit Estonia, which, as we know, was the first state subject to a massive cyberattack from Russia. Are there lessons to be learned from examples like Estonia who have experienced this, or from other countries or businesses?

Admiral Rogers, are there lessons that we should be taking from what's happened in other places?

Admiral ROGERS. It's not by chance that I've been to Estonia twice in the past year. Again, I'm not going to get into specifics, but we have talked about creating a relationship to try to build on it. Although one comment I make to my Estonian teammates also is, what works necessarily in your construct may not——

Senator SHAHEEN. Sure.

Admiral ROGERS.—necessarily scale directly to a nation of 350—you know, 335 million and the largest economy in the world. There are perhaps some things that we can take away from this. Because you have to admire—they sat down and decided this was a national imperative for them, and they consciously sat down and asked themselves, What do we need to do to get where we want to be? Then, how can the government help to be a primary driver in this? Not the only focus, but how can we harness the power of the government and their structure to help drive that? That aspect of it is very impressive, to me.

Senator SHAHEEN. I would agree with that. I was very impressed with what I heard. To follow up on what you're saying, do you think we've reached the point where we believe that this is a national imperative for the United States?

Admiral ROGERS. Intellectually, my sense is, most people intuitively realize that, but then translating that into a series of specific actions to drive broader change than we have done, I think that is still the rub, if you will.

Senator SHAHEEN. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Cruz.

Senator CRUZ. Thank you, Mr. Chairman.

Mr. Secretary, Admiral, thank you for your service. Thank you for joining us today on this vital topic before this committee.

Admiral Rogers, during your testimony to this committee in April, you indicated that the Department of Defense was making significant progress towards establishing 133 Cyber Mission Force teams with plans to be fully operational by the end of fiscal year 2018. In my home State of Texas, I'm very proud of the contributions of the Air Force Cyber Command. I'm glad to see that the Air Force is taking advantage of the unique synergies between the academy, industry, and the military which exist in San Antonio.

The combined efforts of the Air National Guard and the Active Duty Forces at Lackland have played, and will continue to play, an integral role in modern cyber warfare. I thank them for their hard work, and you for your leadership to ensure that they have the right tools they need to train, to fight, and to win.

Admiral Rogers, would you provide an update on the Cyber Mission Force and detail specific shortfalls that merit congressional assistance?

Admiral ROGERS. The Cyber Mission Force, 6,187 individuals and 133 teams focused on three missions, providing capability to provide combatant commanders, if you will, with offensive capability, providing defensive capability to defend the Department of Defense Information Network [DODIN], if you will, the DOD network structure, also the third mission set for us, providing capability to help defend critical U.S. infrastructure against significant acts of cyber consequence, if you will. Three primary mission sets, those 133 teams, if you will, break down into those three different missions.

The first goal we had was IOC of the 133 teams by 30 September of 2016. That's three weeks from now—or two weeks or so from now. We will be IOC by 30 September 2016 of all teams. I would compliment the services, because this is one where, quite frankly, I haven't been the nicest individual, at times, about, what don't we understand about—this is a goal and a standard, and we are going to meet this. We're on track to do that.

The next major milestone, if you will, in the fourth generation, is to be at full operational capability by 30 September 2018, because our experience is that it takes about 2 years to get a team, from the time we stand it up til it's fully mission capable, so the teams we're finishing standing up this month in IOC, we expect it'll take us 2 years to get them to full operational capability.

The biggest challenges meet a continue—we continue to learn insights about tools on the cyber defensive side that we need to continue to deploy more broadly. I'm trying to use a best-of-breed approach to this across the Department, whereas we generate insights from capabilities that the individual services have—NSA, Defense Information Systems Agency [DISA], other elements—let's pick the best of breed, and let's apply it more broadly. Let's not waste money, everybody trying to do their own thing, here.

Investment in the persistent training environment, our ability to actually simulate, in garrison, the networks that we're going to defend, the networks that we're going to operate on. That's fundamental to the future for us. We just cannot afford a model, where we do these major exercises, we try to bring everybody together. It's just a cost-intensive approach to doing business. It's a part of our strategy, but it shouldn't be the fundamental backbone.

Cyber situational awareness is another area where I would argue we have got to be able to visualize this battlespace. Right now, we just don't do that well. I have prioritized it at a lower level. I'm the first to acknowledge that. We've had to identify where can we take risk, so I've tended to prioritize it lower. It's an area where I remain concerned from a—we need to increase the level of investment. We're taking too much risk.

Those are probably the—I don't want to give you a long answer, because I know you have limited time, Senator—those would prob-

ably be the three biggest areas that I would argue we need to keep focused on, keep investing on.

Senator CRUZ. Okay. Thank you, Admiral.

Let me shift to a different topic. An NBC news article this week claims that, despite evidence that Russia is behind a number of cyber intrusions into American networks, that the administration failed to respond because it determined that we need Russia's help in Syria. If true, the Obama administration will have effectively ignored the threats from an adversary, that it is actively trying to influence the election process and will set a terrible precedent for our country, going forward.

Mr. Secretary, are these reports true? Is this, in fact, what the administration's done?

Mr. LETTRE. I'm not aware of the details of that particular NBC story, Senator, but I'm not aware of any linkage of these issues that I've seen in the policy discussions. The incidents that you've described around the apparent hacking related to our electoral systems is under an aggressive FBI investigation so that the U.S. Government can compose its own conclusions about what has occurred there and what are the appropriate actions to take in response. To the discussion that the committee has been having this morning around cyber deterrence, it will be very important to look at the facts around that investigation and the conclusions from it in order to inform policy choices about what kind of acts to take in response.

Senator CRUZ. Very well.

Thank you.

Chairman MCCAIN. Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

Thank you for—both for your service and the excellent contribution that you're making to our national defense.

I want to return to the Chairman's questions about our electoral system. Isn't there a pretty powerful argument that our systems of elections and voting ought to be declared critical infrastructure?

Mr. LETTRE. Senator, that—that's an important question. I think, when we look at critical infrastructure across the country, we do need to consider the possibility of attacks on infrastructure causing significant consequences to the U.S. If there were scenarios where we could envision attacks having significant consequences in our electrical—electoral context, we really do need to consider that.

Senator BLUMENTHAL. Well, certainly we've envisioned those potential consequences.

Admiral, your response to the Chairman's question was, in part, that this electoral system is—I think you used the word "disparate," by which I took it to mean decentralized; "disparate" meaning divided and localized——

Admiral ROGERS. Yes, sir.

Senator BLUMENTHAL.—which is true. Every State has its own system. As you well know, in our presidential elections, the electoral college is the critical decision maker, which results from elective systems within States. Of course, elections have consequences at the State and local level, as well, and now many are driven or directed by some kind of computer collection of information, so they are vulnerable, maybe not at the ballot box, but at some point in

the chain of collecting and assimilating that information. Isn't that troubling to you? I don't know the circumstance of Arizona. You're not familiar with the circumstance of Connecticut, but——

Admiral ROGERS. Right.

Senator BLUMENTHAL.—this is a common thread in our elective system. We've seen, from some of these hacks, that they can have very severe impacts on the—these systems, and they are largely unprotected right now.

Admiral ROGERS. I think it raises a broader question of, What is truly critical in the cyber world? You know, we've tended to think—I think, my sense—we've tended to think along very traditional industrial, in many ways, you know, kinds of lines. One of the things, I think, that the events in the last few years are highlighting to us is that, for example, we need to think about data in a whole different way. What are the implications from a security and a critical infrastructure——

Chairman MCCAIN. Admiral, wouldn't the selection of our leaders—of our system of government be—there should be no discussion about that.

Admiral ROGERS. Senator, my——

Chairman MCCAIN. If you attack that, and succeed in destroying that, you've destroyed democracy.

Admiral ROGERS. So——

Chairman MCCAIN. Why are we equivocating, here, about this? I'm sorry to interrupt.

Senator BLUMENTHAL. No, I——

Chairman MCCAIN.—Senator Blumenthal.

Senator BLUMENTHAL. Mr. Chairman, you took the words, much more eloquently, out of my mouth. I think there is not only a powerful argument, it's virtually incontrovertible.

I understand that you're approaching it from a more abstract standpoint. I don't mean to interrupt, because I'm here to listen to you, but I would hope that there would be a move to designate these systems as critical infrastructure. Why don't you—I know you were remarking on the——

Admiral ROGERS. Yes, sir.

Senator BLUMENTHAL.—nature of data.

Admiral ROGERS. My only point is, if you look at critical infrastructure, from a data perspective, and you look at— What are the key data-driven decisions that tend to shape us of a—as a Nation?—you come to a very different conclusion about an election that—structure—for example, that if your perspective was, "Well, critical infrastructure, to us, is primary industry"—that that's my only point to you, is, this leads us, I think, to a different set of conclusions as to what is truly critical, here. An election system is a good example of that.

Senator BLUMENTHAL. Well, my time has expired, but I think that we really need a national consensus that our electoral system, our system of choosing our leaders, as the Chairman has said very well—our system of choosing leaders at every level, not just the national level, but State government, State legislators—all of these systems are going to be increasingly involving the collection of—you refer to it as "data"—the data are votes. The votes are individual citizens deciding who their leadership is going to be, which

is going to determine who sits in the chair you occupy right now. These chairs here. Who makes these critical decisions. Nothing is more fundamental—our financial system, our utilities, our system of healthcare, all are critical infrastructure. I think our system of electing and choosing leaders is no less so.

Thank you very much.

Chairman MCCAIN. Senator Ernst.

Senator ERNST. Thank you, Mr. Chair.

Gentlemen, thank you very much for coming in today and talking about cybersecurity and its impact on our national security.

I'd like to address some situations from the National Guard perspective. I'm a former soldier in the Iowa National Guard, and I have been tracking the increasing cyber capabilities that both the Army and the Air National Guard are bringing to the table, even in my own home State of Iowa. Unfortunately, it appears that the DOD has not been tracking this as closely as I have.

A report from the Government Accountability Office [GAO] last week stated that, quote, "DOD does not have visibility of all National Guard unit cyber capabilities, because the Department has not maintained a database that identifies the National Guard units' cyber-related emergency response capabilities, as required by law," end quote.

This is a little bit alarming to me, because, in the National Guard, we do have some tremendous capabilities, and we're able to poll a number of those private-sector cyber warriors into the Guard. That's their part-time job and full-time job. They are very talented, and we want to see that they are being used to the fullest of their capabilities.

Admiral, how close is the DOD to having a database of all of the National Guard cyber capabilities required by law?

Admiral ROGERS. Senator, I can't answer to the specifics of the National Guard Bureau. Let me only say this. I am the son of a guardsman. My father was enlisted as an officer in the Illinois Guard for 25 years. This is the world I knew as a child, growing up. The Guard and the Reserve are something personally important to me. In fact, I just, coincidentally, sat down with a team over the last week and were just reviewing, What's the Guard and Reserve plan, the portion of the mission-force piece?

The point I think you make is both important. I'm the first to acknowledge that. I will take an action from here to pull the string on this, because, I apologize, I just haven't seen that report, and I don't know the specifics. It is reflective. We have always maintained that, as we're building the breadth of capability for the Department in cyber, that the structure we have to come up with has to go way beyond just the Active piece, here, that the Guard and Reserve have got to a critical piece of what we do here, which is why, if you look at what the Air Force is doing, six of their 40 or so teams are Guard or Reserve. If you look at the Army, for example, they are bringing online an additional 22 Cyber Protection Teams from the Guard, purely associated with Guard and State missions, not necessarily the Cyber Mission Force, because they realize the importance of this investment. Marine Corps and Navy, there is—their approach, slightly different. Again, they don't have a Guard structure. Their approach, slightly different.

If I could, let me take for action that one and pull the strong. Then I apologize, I just don't——

Senator ERNST. No, I——

Admiral ROGERS.—have a good answer——

Senator ERNST.—I certainly appreciate——

Admiral ROGERS.—for you there.

Senator ERNST.—that. One team, one fight. I think there's a lot of capabilities that we are simply not utilizing or considering when we look at that big picture. I do appreciate that a lot.

[The information referred to follows:]

Responsibility for a DOD database for all National Guard cyber capabilities required by Law is beyond my purview. National Guard response capabilities that are domestic only (title 32 or state Active Duty status and retained by the governor), report their unit's status of forces to the NGB and are tracked directly by Major General James C. Witham, Director, Domestic Operations and Force Development, National Guard Bureau. The General's staff can be contacted at (703) 607–3643 for any inquiries as it relates to title 32 authorities.

The Secretary of Defense has delegated to Commander USCYBERCOM the Directive Authority for Cyberspace Operations and the execution of title 10 cyber missions. Under my U.S. Code Title 10 authorities and responsibilities, I track the status and readiness of 133 Cyber Mission Force teams under my command. Of the 133 teams, three are National Guard activated under title 10 federal mission support. We use DOD's standard Defense Readiness Reporting System (DRRS) to track readiness of our offensive and defensive teams.

Senator ERNST. Are there steps that you think that you can take that would tie together better our Reserve component, our National Guard component? What kind of efforts can you assist with? What we can we assist with?

Admiral ROGERS. I feel comfortable, overall, with the, quote, "Cyber Mission Force." Where I think the broader challenge for us is, What additional level of investment, as a Department and in a State structure, do we think that is appropriate, over and above that? That's probably the biggest focus area for me, working with General Lengyel, about—What should the future be? Then, whatever investments we make in the Guard and Reserve, how do we make sure that they are tied in and aligned with the broader Department effort? We're working this as one team. Because we just can't afford—everybody's out there doing their own thing. That's just not going to get us where we need to be.

Senator ERNST. Right. Absolutely. I agree.

Then, gentlemen, for both of you, please. The Government Accountability Office also found that the yearly cyber exercise, Cyber Guard, failed to focus on emergency or disaster scenarios concurrent to cyber incidents, an area where the National Guard would be very helpful. What efforts—and again, you may not be tied as much into National Guard, but what efforts could you take to improve Cyber Guard for the upcoming year——

Admiral ROGERS. So——

Senator ERNST.—so that we can focus on those——

Admiral ROGERS.—I haven't seen the specifics of the reports, but I will tell you that, not having read it, I'm, quite frankly, a little bit in disbelief, because I would tell you we call it Cyber Guard——

Senator ERNST. Right.

Admiral ROGERS.—for a reason, because it's focus on, How do we exercise, in an annual basis, the integration of the Guard, Reserve, and the Active component with industry? I spend time at that exer-

cise every year. We just did it in June, down in Tidewater. Some members of the committee, in fact, actually came down and observed it.

I'm a little bit perplexed by the basic premise, but I haven't—I apologize, I just haven't seen the specifics.

Senator ERNST. Okay. My time is running out. Again, I think that demonstrates where we do need to put a little more emphasis on our Reserve-component forces and tie those in to our Active Duty component, as well, and really take advantage of the talent that exists out there, make sure that we're exercising their capabilities.

Admiral ROGERS. Yes, ma'am.

Senator ERNST. Thank you very much, gentlemen.

Thank you.

Senator REED [presiding]. On behalf of Chairman McCain, let me recognize Senator McCaskill.

Senator MCCASKILL. Yes. I want to follow up with Senator Ernst's comments. I just came from a tour around Missouri, and I had the opportunity to see the cyber unit at Jefferson Barracks, the Guard cyber unit at Jefferson Barracks in St. Louis, and also the Cyber Warriors at the 139th Airlift Wing at Rosecrans Air Force Base. Both were remarkable. Both surprised me. I was not aware—and I'm not sure, candidly, you're aware—of all these units and what their capabilities are, and what they're doing. What Senator Ernst just said—what was remarkable about the Guard unit in St. Louis was who these people were in their day jobs. We're talking about the very top level of cybersecurity at a Fortune 500 company that has huge needs in this area. Huge needs. I mean, this guy knows more, I would bet, than a huge number of the people that you are commanding within the Active military, in terms of both cyber offense and cyber defense.

I've realized that this is a great opportunity for our Guard to recruit some of the most talented and technically capable people in the private sector, since the vast majority of the networks that we are supporting, in terms of protection in this country, are, in fact, private networks.

I wanted to bring that up with you and ask your opinion about that integration, and particularly as it relates to the lynchpin with the Department of Homeland Security. Because the beauty of the Guard is, it is busy with domestic security as part of their mission, because of the TAG and the involvement of State governments, whether it's a natural disaster or other kinds of problems. It seems to me that utilizing the Guard as the lynchpin between the Department of Homeland Security and the Department of Defense would make a great deal of sense, Admiral Rogers. I would like your comment on that.

Admiral ROGERS. First of all, I agree with the fundamental premise that the Guard and the Reserve bring a lot of capability. That's one reason why the Cyber Mission Force idea is predicated as the idea—it's our ability to bring it all together—not just all Active, not just Guard; it's the ability to bring it together.

In terms of who should be the fundamental lynchpin—before I get into publicly endorsing a particular strategy or solution, this is just one I want to make sure we think our way through. Because

in—there are challenges if you do it Active-only. There's challenges if you do it over Guard- or Reserve-only. I'd also be interested: Hey, what's DHS's perspective in this?

One of the other challenges I've found so far in my time in command, we have to work our way through what—and this is where the Guard, I think, becomes incredibly critical—what's the difference between—we're using DOD capability to work Federal large critical infrastructure versus what is the capability DOD—by extension, the Guard—can bring to the fore at a much more localized State and local level? That's an area that, clearly, the Guard is very optimized for, that the Active piece is not as readily optimized for.

Senator MCCASKILL. I'm sure one of our problems in this space is retaining Active personnel, because if they become very skilled in this area, the—there's lots of lucrative opportunities in the private sector. Has there been any thought given to an Active recruitment of these folks into the Guard as they move into the private sector for a lot more money and people not being able to tell them where they're going to live 24/7? Is it possible that we are losing an opportunity, in terms of retaining some of the talent that we have, by not directly recruiting them into the Guard?

Admiral ROGERS. Knock on wood, retention on the Active side is exceeding our expectations. That doesn't mean it won't change tomorrow or next week or next month.

I will say, since the Guard is an Air Force and an Army-specific construct, I know both of those services, in my discussion with my subordinate commanders from them, talk about, how do we make sure, as we're watching the workforce transition out of the Active—separate, retire—is there a way to tie in the Guard piece? Senator Cruz mentioned San Antonio, for example. I've seen several instances in the San Antonio area, because they're such a large concentration, where this is working very well. I'm not sure how well it's working in those areas where we don't have this large Guard and Active——

Senator MCCASKILL. Right.

Admiral ROGERS.—complement of force, if it will. I just don't know, off the top of my head.

Senator MCCASKILL. This idea has been discussed openly, and I know there is a lot of controversy around it and a lot of pros and cons, but one of these really talented cyber warriors at the Guard unit that I visited with, I was told that one of them almost was removed because of sit-ups. What about the PT requirement? What value is there to forming an elite cyber squad that is civilian, as opposed to, you know, losing a really talented guy because of sit-ups?

Admiral ROGERS. My first comment would be, remember, the Law of Armed Conflict specifically prescribes what civilians and uniforms can do in some particular applications. I generally remind people, a lot of it would have to do with, what would the mission be that you gave that entity? Because there are some things in the Law of Armed Conflict that physically could not do. Uniforms have to do it, as opposed to——

Senator MCCASKILL. Right.

Admiral ROGERS.—application of force and capability.

To date, are there numbers where that is an issue? Clearly. I'm not going to pretend, for one minute. We have been able to retain people and still meet the requirements associated with the broader military without decreasing capability. If that changes over time, though—it's one of the things I have talked about—we need to be mindful that if circumstances change, we need to look about changing the rules that we currently operate. If the situation were to change, those would be one of the things I would say, "Do we need to look at a different force balance or mix? Do we"——

Senator MCCASKILL. Right.

Admiral ROGERS.—"need to look at a different set of standards or requirements associated with individuals?" I don't think we're at that point now, but if the situation were to change, I think we would definitely need to do that.

Senator MCCASKILL. I would certainly urge that flexibility——

Admiral ROGERS. Yes, ma'am.

Senator MCCASKILL.—because I think this is going to be a growing part of our national security——

Admiral ROGERS. Right.

Senator MCCASKILL.—piece.

Admiral ROGERS. Thank you.

Senator REED. On behalf of the Chairman, let me recognize Senator King.

Senator KING. Thank you, Mr. Chairman.

It seems to me the good news is that we're the most wired society on Earth. It gives us fantastic efficiencies and productivity and advantages, in many ways. The bad news is, we're the most wired society on Earth, which means we are the most vulnerable.

Admiral Rogers, you're familiar, I'm sure, with the Ukraine hack of the grid in December 2015. One of the things we learned from that is that there—that hack was much less serious than it might have been, because of some retro technology——

Admiral ROGERS. The antiquated——

Senator KING.—analog switches, old Demetri, who had to go out and throw a switch somewhere at a relay. Do we have some lessons from that, that we ought to be thinking? Thinking about elections, it's hard to hack a paper ballot.

Admiral ROGERS. Sir.

Senator KING. Those kinds of things. Is that—should we be examining that area?

Admiral ROGERS. I mean, we certainly are. I mean, one of the lessons, I think, from the Ukraine, for example, is, not only the analog, the physical piece, but also the way that their grid was broken down into components.

Senator KING. Right.

Admiral ROGERS. It's leading to some things. For example, as a naval officer, we're teaching celestial navigation again——

Senator KING. I was going to bring that up.

Admiral ROGERS.—at the Naval Academy.

Senator KING. I understand it's the first time in 20 years that——

Admiral ROGERS. Right, which we had stopped doing, because we said to ourselves, "Well, we have automated chart processes now.

Why would we need to use celestial bodies to—for navigation to define out"——

Senator KING. Because you can't hack a sextant.

Admiral ROGERS. Yes, sir. We acknowledge that there are things that we are going to need to look back, in this current world we're living in, and say to ourselves, "Perhaps some of the assumptions that we've made are not going to prove to be accurate." We've got to ask ourselves, "What are the second- and third-order implications? What have we got to train differently? What skills do we need to have that we perhaps"——

Senator KING. We also need to——

Admiral ROGERS.—"for the last 20 years have said we don't need?"

Senator KING. As you—as I think you've said, we need to question the basic assumption that digital is——

Admiral ROGERS. Yes, sir.

Senator KING.—always better.

Admiral ROGERS. Yes, sir.

Senator KING. Senator Risch and I have a bill in before the Energy and Natural Resources Committee to ask the National Labs to work with the utilities to look at the Ukraine situation and see if there are places—not to de-digitize the——

Admiral ROGERS. Sir.

Senator KING.—grid, but places where there could be analog switches or other devices put in to deal with just——

Admiral ROGERS. Right.

Senator KING.—just this issue.

Let me turn to encryption for a minute. While this hearing was going on—and I don't want to sound like this was a big production—in about, literally, a minute and a half, I downloaded Telegram. Telegram is an app, as you know, that's encrypted. I thought it was interesting. I looked at what it—how it works. It's fully encrypted. It's in English, Arabic, Dutch, German, Italian, Korean, Portuguese, and Spanish. It's—was started by two brothers from Russia. It's based in Berlin. I mean, this is the reality, isn't it, Mr. Lettre, that we're—we can't stop this. The idea of somehow being able to control encryption is just not realistic.

Mr. LETTRE. We can't stop these trends, you're right, Senator. Individuals—all of us benefit from strong encryption. The Department of Defense does. I personally am in favor of having strong encryption that allows me to protect my personal data. The challenge is—and yet, we need to find our—think our way through how we can continue to fulfill our responsibilities to enforce the laws and protect the Nation. I think what we do find is, there are a number of instances where government leaders have been able to strike a very collaborative and cooperative dialogue with key sectors in the text sector. Individual players and executives have been able to focus on finding——

Senator KING. That——

Mr. LETTRE.—solutions.

Senator KING.—that worked pretty well in the '20s, when you were talking about the telephone system, which was only within the country. You can—we can deal with Apple or with Microsoft or with Cisco or whoever, but if you've got a cloud-based app that's—

the headquarters is in Berlin, and who knows where the data is—I mean, we—as hard it is for us to believe, there are places our power doesn't reach. We can't regulate something that's over in Berlin or Swaziland.

Mr. LETTRE. That's a very good point. There will always be places across these sectors and these technology solutions that we just—we may not be able to find a way forward. They may be—the solution may be elusive.

Senator KING. Well, I'd like——

Mr. LETTRE. It does require us to think innovatively—Senator KING. Well——

Mr. LETTRE.—even beyond encryption, about how we can continue to go after national security challenges.

Senator KING. That was—you know, the word "innovation"—I mean, this is a—this is the world history of conflict, is invention, reinvention, reinvention, reinvention.

I also want to associate myself with Senator Lee's questions. We also need to get back to old-fashioned human intelligence. I think it's—SIGINT [Signals Intelligence] was easy, in a sense, if you can pick up conversations. Now that that's no longer as easy as it once was, we need to be thinking about, what are the other techniques that we can use? They—and it may be old-fashioned intelligence. It may also be other high-tech satellite or other things. It—it's—we can't—I think innovation is going to be an absolute key to this.

Mr. LETTRE. Yes. That's absolutely right, Senator. The—in particular, as you pointed out, we do need to build innovation across a range of intelligence disciplines and collection capabilities. Even in the human intelligence arena, we know how effective it can be. We also know that technology trends are changing how we do HUMINT [Human Intelligence]. We need to be able to adapt and invest in innovation, in how we conduct our human intelligence operations, as well.

Senator KING. My time is up, but I would suggest big data analysis is one of those tools.

Mr. LETTRE. Absolutely.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Senator REED. Thank you, Senator King.

On behalf of the Chairman, let me thank you gentlemen for your testimony today and your service.

Since there are no other colleagues here, I would call the hearing adjourned.

Thank you.

[Whereupon, at 11:20 a.m., the hearing was adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR ROGER F. WICKER

ZTE

Senator WICKER. The Commerce Department announced on March 8 that it had added ZTE to its entity list for setting up shell companies in order to ship equipment that contained U.S. parts to Iran. However, Commerce later softened the sanctions against ZTE and allowed U.S. companies to temporarily ship goods to ZTE, and has extended this temporary license several times, most recently through November 28.

In addition to having a history of evading U.S. sanctions, ZTE, and other Chinese telecommunications firms like Huawei and Lenovo present a potential cyber security risk to U.S. national security. There have been numerous instances where the U.S. Government, through the CFIUS process, has canceled mergers between American companies and these Chinese telecommunication firms. Additionally, there have been many statements and reports on the risks these companies present, ranging from the 2012 House Permanent Select Committee on Intelligence report on "U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE" to comments by former CIA Director and NSA Director General Michael Hayden who stated that Huawei had "shared with the Chinese state intimate and extensive knowledge of foreign telecommunications systems it is involved with."

ZTE and Huawei obviously present a national security risk.

1. Do you think that the Defense Department should be using technology that includes component parts or software from Huawei, ZTE, or other Chinese telecommunication companies?

Mr. LETTRE. Decisions to use technology from Huawei, ZTE, or other Chinese telecommunication companies must be made on case-by-case basis using a risk-based methodology. DOD does not "blacklist" suppliers or individual products, except as directed by law (e.g., munitions list items, countries promoting terrorism). DOD does, however, create Approved Product or Supplier Lists (Whitelists) of products or organizations that have been assessed for use in certain applications. There are currently no Huawei or ZTE products on the DOD Unified Capabilities Approved Products List (APL). The fact that a product does not appear on an APL does not mean contractors cannot offer bids or that the government can still select outside the APL. It's the policy of the DOD to solicit from a broad number of potential offerors and award contracts based on full and open competition to the maximum extent possible.

Short of suspension and debarment, federal contractors and vendors are not precluded from competing on DOD contracts.

It is important to note that the Department has several mechanisms in place to help ensure the security of products or services delivered to us and the systems used to store or process sensitive DOD information. For DOD national security systems, there are program protection planning (DOD Instruction (DODI) 5000.02) and supply chain risk management (SCRM; DODI 5200.44) policies and processes which require programs to identify critical components and request threat reports on them from the Defense Intelligence Agency's SCRM Threat Analysis Center. DOD mitigates identified risk where possible, but also has authorities granted by section 806 of the NDAA for FY 2011, as amended by section 806 of the NDAA for FY 2013, which enables DOD components to exclude a source that fails to meet established qualifications standards or fails to receive an acceptable rating for an evaluation factor regarding supply chain risk for information technology acquisitions, and to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source. [1]

Admiral ROGERS. As this question concerns a Department of Defense-wide position on technology acquisitions and use, it exceeds the scope of my direct responsibility, but from my unique understanding and knowledge on the issues at stake, I join in the response submitted by Mr. Lettre, USDI, to this same question.

[1] NSA avoids the use of products from vendors with a disqualifying Foreign Ownership, Control or Influence (FOCI), in accordance with its security and Information Awareness policies. The Agency makes decisions regarding acquisitions from FOCI vendors and acceptance of their goods and services on a case-by-case basis. In particular, the Agency requires vendors and potential vendors to disclose FOCI, and evaluates these disclosures in its acquisition decisions. The Agency may require vendors to produce an appropriate mitigation plan or substitution of products for items produced or services performed outside the United States or its territories.

2. Senator WICKER. Are there any parts, components, software, products, or other related items from any Chinese firm, including Huawei, ZTE, or Lenovo, present in the Defense Department unclassified and classified information technology (IT) network, telecommunications network, and related infrastructure? (For the purposes of this question, the IT network, telecommunications network, and related infrastructure includes, but is not limited to, fiber optic cables, computer chips, software, personal computers, office desktop computers, servers, routers, telecommunications equipment, and networking equipment, at any State Department location in the United States or around the world.)

Mr. LETTRE. Yes, there are parts/components/software/products from Chinese firms in DOD's unclassified and classified networks, telecommunications, networks and related infrastructure. Most products used by the USG, including DOD, have component parts manufactured in China. In addition, DOD systems and networks sometimes use products from Chinese firms. Decisions for inclusion of components from Chinese firms or with nexus with China (such as manufacturing or test) are made on a case-by-case basis based on an assessment of risk specific to the system.

The Department leverages several mechanisms to enable it to manage supply chain and cybersecurity risks to its systems and networks, while cost effectively leveraging globally sourced technologies.

First, the Department requires Program Protection Plans (PPPs) to address the full spectrum of security risks for the critical components contained in our national security systems, including supply chain vulnerabilities, and to implement mitigations to manage risk to system functionality. Within program protection planning, DOD performs criticality analysis to identify critical components for added protections. Such components are subjected to all source intelligence evaluation and, where risks are identified, vulnerability analysis.

There are additional statutory authorities available to the Department to limit or exclude vendors in specific circumstances. For example, section 1211 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2006, as amended by section 1243 of the NDAA for FY 2012, and as implemented at DFARS section 225.77, prohibits the Secretary of Defense from acquiring supplies or services that are on the United States Munitions List through a contract, or subcontract at any tier, from any Communist Chinese military company. In addition, section 806 of the NDAA for FY 2011, as amended by section 806 of the NDAA for FY 2013, has been implemented at DFARS Subpart 239.73, "Requirements for Information Relating to Supply Chain Risk." The clause enables DOD components to exclude a source that fails to meet established qualifications standards or fails to receive an acceptable rating for an evaluation factor regarding supply chain risk for information technology acquisitions, and to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source.

Admiral ROGERS. As this question concerns a Department of Defense-wide position on technology acquisitions and use, it exceeds the scope of my direct responsibility, but from my unique understanding and knowledge on the issues at stake, I join in the response submitted by Mr. Lettre, USDI, to this same question.

CHINA

Senator WICKER. In his testimony before the Senate Armed Services Committee on February 9, 2016, Director of National Intelligence James Clapper labeled China a "Leading Threat Actor" in regards to cyber threats. Specifically, the he stated in his written testimony: "China continues to have success in cyber espionage against the U.S. Government, our allies, and U.S. companies. Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy. We will monitor compliance with China's September 2015 commitment to refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property with the intent of providing competitive advantage to companies or commercial sectors. Private-sector security experts have identified limited ongoing cyber activity from China but have not verified state sponsorship or the use of exfiltrated data for commercial gain."

3. Senator WICKER. Do you agree with his assessment that China is a "Leading Threat Actor" and that China "continues to have success in cyber espionage against the U.S. Government, our allies, and U.S. companies"?

Mr. LETTRE. Yes.

Admiral ROGERS. Yes.

QUESTIONS SUBMITTED BY SENATOR KELLY AYOTTE

PROTECTING IRAN'S NUCLEAR PROGRAM FROM SABOTAGE

Senator AYOTTE. As I mentioned in your April hearing, according to paragraph 10.2 of Annex III of the Joint Comprehensive Plan of Action (JCPOA), or 'Iran Deal', the U.S. must cooperate with Tehran "through training and workshops to strengthen Iran's ability to protect against . . . sabotage" of its nuclear program. I asked you, from a cyber perspective, has the U.S. helped Tehran strengthen its ability to protect against sabotage of its nuclear program. You said that U.S. Cyber Command has not participated in any such efforts.

4. Is this still accurate?
Admiral ROGERS. Yes.

5. Senator AYOTTE. Are you aware of ANY U.S. government activities helping Iran protect its nuclear program against sabotage?
Admiral ROGERS. No.

ECTR FIX

Senator AYOTTE. I understand that there is an important division between the FBI's domestic law enforcement and your mission.

6. However, based on your experience, are you familiar with the Electronic Communications Transaction Records, or "ECTR fix" that the FBI has identified as a top priority in terrorism investigations?
Admiral ROGERS. I do not have sufficient knowledge about the "ECTR fix" to comment on it.

7. Senator AYOTTE. Would you agree that ensuring that law enforcement has the tools they need to prevent future attacks is extremely important?
Admiral ROGERS. I agree with the general proposition of the question that it is important that law enforcement have access to necessary tools. However, speaking from my roles as the Commander of U.S. Cyber Command and Director of NSA, there are many factors that we take into consideration when evaluating whether to pursue the use of a specific tool, chief among them that it is consistent with law and policy.

8. Senator AYOTTE. Do you agree that providing law enforcement with the authority to appropriately obtain basic information—excluding content—is extremely valuable in helping to piece together actionable intelligence that can help stop an attack?
Admiral ROGERS. I agree with the general proposition of the question that non-content data could be of great use to law enforcement in any given investigation. Speaking from my roles as the Commander of U.S. Cyber Command and Director of NSA, this type of information is certainly of value.

9. Senator AYOTTE. Based on your experience, do you agree with FBI Director Comey's assessment that the ECTR fix "would be enormously helpful?"
Admiral ROGERS. As I noted earlier, I do not have sufficient knowledge about the "ECTR fix" to comment on it.

CHINA

Senator AYOTTE. The U.S and China entered into a Cyber theft agreement in September 2015. China pledged that their government would refrain from computer—related theft of intellectual property for commercial gain.

10. Senator AYOTTE. Has China honored that commitment? If not, what have we done about their failure to honor their commitment?
Admiral ROGERS. [Deleted.]

11. Senator AYOTTE. If not, what is your assessment of Chinese cyber activity since then? What have they been doing? Are these activities directly or indirectly conducted or supported by the Chinese government?
Admiral ROGERS. See answer to question ten.

12. Senator AYOTTE. Does China continue to target and exploit U.S. government, defense industry, and academic networks?
Admiral ROGERS. Yes.

13. Senator AYOTTE. How confident are we that these intrusions, thefts, and attacks from China are coming from government or government-supported sources (as opposed to private Chinese actors not acting in cooperation with the government)?
Admiral ROGERS. [Deleted.]

IRAN'S CYBER ACTIVITIES

14. Senator AYOTTE. Can you describe Tehran's current cyber capabilities and activities? How have Iran's cyber activities and capabilities changed since the adoption of the Iran Deal?
Admiral ROGERS. [Deleted.]

NORTH KOREA'S CYBER ACTIVITIES

15. Senator AYOTTE. Can you describe North Korea's cyber capabilities and activities? How does North Korea use these capabilities and activities in furtherance of its nuclear and ballistic missile programs?
Admiral ROGERS. [Deleted.]

IDENTITY MANAGEMENT

16. Senator AYOTTE. How is DOD improving identity management and data access? What is your view of enhancing identity management and data access by incorporating improvements to authentication, accountability, privacy, and deployability?
Secretary LETTRE. The Department of Defense (DOD) is taking aggressive action to improve identity management and data access capabilities. These capabilities, which are critical to military operations and defense activities, are foundational components of DOD's Information Assurance Program and enable secure information sharing within DOD and with mission partners. DOD is also working to address privacy concerns and to ensure protection of civil liberties as it implements stronger authentication and authorization on sites accessed by consumers, retirees, family members, businesses, and home users.

Improving authentication and authorization policy, processes, capabilities, and adoption reduces overhead and costly information sharing friction, and improves accountability and access to data resources. To that end, DOD has identified that mission partner interoperability is only possible if we coordinate our identity policies and standards around industry norms. DOD supports the Office of Management and Budget's (OMB) Identity, Credentialing, and Access Management for standardization across the federal government—including the Intelligence Community—and resulting National Institutes of Standards and Technology (NIST) draft special publication on Digital Authentication Guidelines. DOD is leveraging this same standardization effort in its dialogue with Allies and industry partners, oriented on the same goals.

DOD is also working with OMB and General Service Administration (GSA) to improve trust, security, and privacy support on commercial devices and browsers off the shelf. By making changes to the Federal and DOD Public Key Infrastructure (PKI) that supports our websites, we intend to eliminate trust errors that have been a frustration for users outside of DOD networks.

DOD is also undertaking a two-year effort to diminish our reliance on the Common Access Card (CAC) as the only acceptable way to authenticate on many DOD IT systems. Broadening DOD authentication support has two main objectives. First, to improve interoperability with mission partners—many of whom have not chosen to implement smart card authentication; and second, to support strong authentication on emerging devices like smartphones and tablets that the CAC has simply not been able to support.

As part of this effort, DOD is working with OMB to converge around standards for "derived credentials" that can be supported securely by current and future commercial smart phones and tablets. Supporting the Personal Identity Verification (PIV) standard capability ("CAC" for DOD) by implementing a virtual card on DOD's half-million mobility devices will significantly improve information sharing capability for our forces on the move. Supporting mobility with high-assurance authentication will significantly enhance deployable access and lower the risk of making more mission data available at the point of need.

DOD Acquisition Programs are working to leverage existing and emerging strong authentication capabilities for implementation on deployable systems, and researching alternatives that support specific operational environments or device form factors. The SECDEF's top priority within the Cybersecurity Discipline Implementation Plan is implementation of strong authentication and elimination of authentication solely by username-password. Within that effort, the early focus is on mission

systems and applications where compromised credentials would pose the most risk—including users with powerful administrator-level privileges across our networks.

DOD is also leveraging the SECDEF's Defense Innovation Unit Experimental to identify innovations in industry that we can quickly adopt to close additional gaps in our authentication capabilities. We're working to identify fair, open, and transparent means to identify industry innovation in the authentication area.

Stronger authentication and rules-based authentication is critical to advancing privacy protections across the DOD—particularly in response to the Office of Personnel Management (OPM) breach last year. DOD is working to leverage our most advanced access control technologies to protect this data and other sensitive datasets—especially large stores of Personally Identifiable Information (PII). By shifting from legacy account management to enterprise identity and access control capabilities, we can reduce the exposure of PII on local systems to support administration of user access. DOD is also working to improve monitoring and audit for users that have access to sensitive data to identify abuse by authorized personnel, and to identify credentials that have been compromised.

Consistent with the Cyber National Action Plan, DOD intends to implement multi-factor authentication and forced session encryption for consumers that access personal information on DOD websites. We're working with OMB and GSA to identify how DOD can leverage capabilities across the federal government to meet those requirements, understanding that consumers using DOD systems will invariably require strong authentication access to other federal resources.

CHIEF DATA SCIENTIST

17. Senator AYOTTE. In 2015 the White House named the first-ever "Chief Data Scientist." What is your view of creating a Chief Data Scientist position within the DOD?

Mr. LETTRE. DOD does not currently have a Chief Data Scientist position. However, depending on future DOD requirements, the creation of a DOD Chief Data Scientist position may be considered.

QUESTIONS SUBMITTED BY SENATOR MIKE LEE

Senator LEE. Some officials believe that commercial companies should build into their products "back-door" systems or other similar mechanisms that enable the government to access encrypted information on personal communication devices when doing so is deemed necessary for protecting the nation's security. However, building such openings into products like smart phones will leave them vulnerable to the types of cyber-security threats that we are also seeking to prevent. Writing in the Washington Post in July 2015, former NSA Director Mike McConnell and former DHS Secretary Michael Chertoff stated [QUOTE] "If the United States is to maintain its global role and influence, protecting business interest from massive economic espionage is essential."

18. What sort of economic and security risks could companies face if they are compelled to build "back-doors" or other vulnerabilities in their products and systems?

Admiral ROGERS. There are any number of legitimate considerations in the debate over encryption, to include economic and security risks to our private sector. However, there are companies that for business purposes currently provide for their own access to encrypted data sent by users of their products and they are presumably doing so with those economic and security considerations in mind. As such, it does not necessarily follow that lawful access by one entity implies unlawful access for an unauthorized entity. Thus, consideration for whether to ensure a product allows for lawful access needs to balance the government's duty to ensure public safety and conduct foreign affairs with any increased risks to the security of the device. I believe the debate over encryption should take into account these and all other legitimate considerations—including the importance of this data to law enforcement and national security matters—and that this issue can only be solved by cooperation between the government and the private sector.

19. Senator LEE. Since you are tasked both with protecting vulnerable systems and enabling our military and intelligence forces to detect threats, how do you reconcile the tension between these two missions?

Admiral ROGERS. These missions are inherently complementary and mutually supportive.

20. Senator LEE. Requiring U.S. companies to provide access to government agencies would not prevent foreign app developers from creating encryption software for jailbreak phones. Wouldn't the logical response for anyone seeking to threaten the United States be to use a foreign encrypted app; thus harming U.S. companies and not giving us any discernable security edge?

Admiral ROGERS. I do not think there exists a simple direct correlation as suggested in the question. There are any number of considerations that go into an individual's decision to use a particular information technology product, service or application. While security is likely one such consideration for many individuals, it is also not likely the only one and, when considering security, the alternative to lawful access by the U.S. government under narrow circumstances may be more appealing than a foreign product subject to potentially unchecked foreign government access.

21. Senator LEE. The FBI was able to access the phone of San Bernardino shooter Syed Farook without the cooperation of the company that created his phone. Secretary Lettre, while I am sure that the specifics of how the FBI accomplished that cannot be fully discussed in an open setting, can you confirm whether similar capabilities are available to the Department of Defense or Intelligence agencies that do not require commercial companies to engage in practices they see as unethical or dangerous to themselves and their customers?

Mr. LETTRE. I cannot answer this question in an open session.

QUESTIONS SUBMITTED BY SENATOR MIKE ROUNDS

Senator ROUNDS. During the Sep. 13, 2016 SASC hearing, you stated the following in response to the question, "Do we have a plan in place today to respond to an attack on critical civilian infrastructure?" Response—"I believe we do have a plan in place, Senator."

22. Would you please provide the plan you referred to in your response? Specifically, I seek a plan prescribing the department's response to an attack on critical civilian infrastructure, not a process-related policy, e.g. PPD–41. If the plan is classified, please so state. Additionally, if the plan's dissemination is restricted, please so state to include the level of classification and access categories, e.g. TS SCI, SAP etc.

Mr. LETTRE. Overall, the Department of Defense's primary concern is defending the United States and its interests, against cyber attacks of significant consequence. DOD's approach to defending the Nation from a significant cyber incident is the same as its approach to defending the Nation in any other domain.[2] Options to directly respond to an adversary cyberattack are not necessarily limited to cyberspace, and DOD considers the full range of military options when providing options to the President.

For domestic cyber incident response, DOD follows the structure put in place under PPD–41 by supporting the incident response activities of the Department of Homeland Security and the Department of Justice, just as we are able to provide support to civil authorities in other domains. As directed by PPD–41, DHS is in the process of finalizing an update to the National Cyber Incident Response Plan (NCIRP).[3] Just as DOD aligns its physical emergency plans with the National Response Framework, it's cyber response plans will align with the framework established under the NCIRP.

---

[2] The recently released Presidential Policy Directive on United States Cyber Incident Coordination (PPD–41) codifies the policy that governs the Federal government's response to cyber incidents. PPD–41 defines a "significant cyber incident" as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[3] The recently released Presidential Policy Directive on United States Cyber Incident Coordination (PPD–41) codifies the policy that governs the Federal government's response to cyber incidents. PPD–41 directs the Secretary of Homeland Security, in coordination with the Attorney General, the Secretary of Defense, and the Sector-Specific Agencies, to submit a National Cyber Incident Response Plan (NCIRP) to the President. Consistent with PPD–41 and the Homeland Security Act of 2002, as amended, the Department of Homeland Security (DHS) is currently coordinating an update to the Interim NCIRP from 2010. DHS has worked closely with both public and private sector stakeholders over the summer to ensure wide participation and input into the development process of the new NCIRP. Hence, they would be in the best position to discuss the plan for responding to an attack on critical civilian infrastructure. The draft plan was recently released for public comment and can be found online at: https://www.us-cert.gov/ncirp.

Not only does DOD plan for these activities, we also exercise them. DOD's Cyber Guard exercise program brings together partners from across government, industry, and the international community to test operational and interagency coordination, as well as tactical-level operations to protect, prevent, mitigate, and recover from a domestic cyberspace incident.

That said, while we plan for a variety of response options, there is no prescribed response plan. Each cyber incident must be assessed on a case-by-case basis to ensure the response is appropriate and communicates the desired message to the adversary.

QUESTIONS SUBMITTED BY SENATOR RICHARD BLUMENTHAL

CRITICAL INFRASTRUCTURE

23. Senator BLUMENTHAL. What are we doing to protect our critical systems—like the electric grid and transportation networks—from cyberattacks?

Mr. LETTRE. Consistent with the Presidential Policy Directive on National Preparedness (PPD–8), PPD–21 on Critical Infrastructure Security and Resilience, and Executive Order 13636 on Improving Critical Infrastructure Cybersecurity, it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial entities, and public and private owners and operators of the critical infrastructure. The Department of Homeland Security provides strategic guidance to a national unity of effort.

Therefore, it is my understanding that the primary effort is to strengthen the security and resilience of our critical systems for the continuity of national essential functions and to organize itself to partner effectively with, and add value to, the security and resilience efforts of critical infrastructure owners and operators. For additional detail, I will defer to DHS.

Admiral ROGERS. [Deleted.]

CYBER ACTS OF WAR

24. Senator BLUMENTHAL. Has the Department of Defense identified what constitutes an act of war in the cyber realm?

Mr. LETTRE. The determination of what constitutes an "act of war" in or out of cyberspace, would be made on a case-by-case and fact specific basis by the President. There would likely be an accompanying assessment of seriousness of a particular cyber activity and potential response options that would be legally available.

Specifically, cyber attacks that proximately result in a significant loss of life, injury, destruction of critical infrastructure, or serious economic impact should be closely assessed as to whether or not they would be considered an unlawful attack or an "act of war." Similarly, the USG would assess malicious cyber activities that threaten our ability to respond as a military, threaten national security, or threaten national economic collapse . . . hence the context for these events is important, and cyber activities should not be viewed in isolation.

Another question the Department is often asked is when does a cyber attack trigger an act of war? Each of those would be discussed in turn, depending on the type of attack or malicious cyber activity and what were the consequences. As of this point, we have not assessed that any particular cyber activity on us has constituted an act of war.

Admiral ROGERS. We concur with the comments submitted by Mr. Lettre, USDI.

25. Senator BLUMENTHAL. What types of actions would the Department of Defense consider to be acts of war in the cyber realm?

Secretary LETTRE. Actions that threaten our ability to respond as a military, threaten national security, or threaten national economic collapse. Each of these would be discussed in turn, depending on the type of attack or malicious cyber activity and what were the consequences. (See Question 24 for more detail)

Admiral ROGERS. We concur with the comments submitted by Mr. Lettre, USDI.