

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

October 20, 2017

The Honorable Robert Kolasky
Acting Deputy Under Secretary
National Protections and Programs Directorate
Department of Homeland Security
Washington, DC 20528

Dear Acting Deputy Under Secretary Kolasky:

Last month, the Department of Homeland Security reportedly notified election officials in 21 states that Russian government hackers had targeted those states during the 2016 election.¹ We are writing to request copies of these notifications and additional documents, as well as a briefing from top Department officials on these matters.

The Department's notifications to these states came nearly a year after the election and three months after the Department publicly disclosed that individuals connected with the Russian government sought to hack voter registration files and public election sites in 21 states.² They also came after numerous other reports that Russia engaged in a multifaceted campaign to disrupt the 2016 election, including widespread cyber-attacks on state-election infrastructure systems.³

The Department's recent convening of the Government Coordinating Council for the Election Infrastructure Subsector, with representatives from the Election Assistance Commission, the National Association of Secretaries of State and state and local election officials, will hopefully facilitate the sharing of information and expertise.⁴

¹ *DHS Tells States About Russian Hacking During 2016 Election*, Washington Post (Sept. 22, 2017) (online at www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.55b916d66ca3).

² *Russians Tried to Hack Election Systems in 21 States, U.S. Officials Say*, Chicago Tribune (June 21, 2017) (online at www.chicagotribune.com/news/nationworld/ct-homeland-security-chief-intelligence-panel-20170621-story.html).

³ See, e.g., Department of Homeland Security, *Joint Analysis Report: GRIZZLEY STEPPE—Russian Malicious Cyber Activity* (Dec. 29, 2016) (online at www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf); Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (Jan. 6, 2017) (online at www.dni.gov/files/documents/ICA_2017_01.pdf).

⁴ Department of Homeland Security, *DHS and Partners Convene First Election Infrastructure Coordinating Council* (Oct. 14, 2017) (online at www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council).

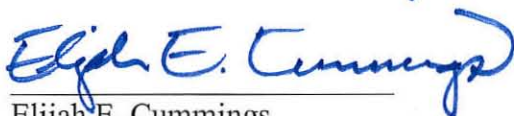
We request that you produce, by October 31, 2017, copies of the notifications sent by the Department to these 21 states, as well as all accompanying materials relating to Russian government-backed attempts to hack state election systems.

We also request a briefing from appropriate Department officials within the same timeframe on the following issues:

- (1) the types of voting equipment that were attacked;
- (2) the timeline by which the Department provided information to these states and the reasons for not sharing additional information sooner;
- (3) services and trainings offered to states to detect and prevent cyber-attacks;
- (4) plans to work with states to detect and prevent future cyber-attacks; and
- (5) the operational plans and goals of the newly convened Election Infrastructure Coordinating Council.

If you have any questions, please contact Jennifer Daehn with the Democratic Committee staff at (202) 225-5051. Thank you for your consideration of this request.

Sincerely,



Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform



Robin Kelly
Ranking Member
Subcommittee on
Information Technology

cc: The Honorable Trey Gowdy, Chairman
Committee on Oversight and Government Reform

The Honorable Will Hurd, Chairman
Subcommittee on Information Technology

RANSOMWARE

What It Is and What To Do About It



WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

HOW DO I PROTECT MY NETWORKS?

A commitment to cyber hygiene and best practices is critical to protecting your networks. Here are some questions you may want to ask of your organization to help prevent ransomware attacks:

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

HOW DO I RESPOND TO RANSOMWARE?

Implement your security incident response and business continuity plan. It may take time for your organization's IT professionals to isolate and remove the ransomware threat to your systems and restore data and normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact law enforcement immediately. We encourage you to contact a local **FBI**¹ or **USSS**² field office immediately to report a ransomware event and request assistance.

There are serious risks to consider before paying the ransom. We do not encourage paying a ransom. We understand that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. As you contemplate this choice, consider the following risks:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
- Some victims who paid the demand have reported being targeted again by cyber actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

¹ https://www.fbi.gov/contact-us/field/listing_by_state

² <http://www.secretservice.gov/contact/>



How to Protect Your Networks from

RANSOMWARE

This document is a U.S. Government interagency technical guidance document aimed to inform Chief Information Officers and Chief Information Security Officers at critical infrastructure entities, including small, medium, and large organizations. This document provides an aggregate of already existing Federal government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.



Protecting Your Networks from Ransomware

Ransomware is the fastest growing malware threat, targeting users of all types—from the home user to the corporate network. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. There are very effective prevention and response actions that can significantly mitigate the risk posed to your organization.

Ransomware targets home users, businesses, and government networks and can lead to temporary or permanent loss of sensitive or proprietary information, disruption to regular operations, financial losses incurred to restore systems and files, and potential harm to an organization's reputation.

Ransomware may direct a user to click on a link to pay a ransom; however, the link may be malicious and could lead to additional malware infections. Some ransomware variants display intimidating messages, such as:

“Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a \$100 fine.”

“You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently encrypted and no one will be able to recover them.”

What is Ransomware?



Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion. Ransomware is frequently delivered through spearphishing emails. After the user has been locked out of the data or system, the cyber actor demands a ransom payment. After receiving payment, the cyber actor will purportedly provide an avenue to the victim to regain access to the system or data. Recent iterations target enterprise end users, making awareness and training a critical preventive measure.

Protecting Your Networks

Educate Your Personnel

Attackers often enter the organization by tricking a user to disclose a password or click on a virus-laden email attachment.

Remind employees to never click unsolicited links or open unsolicited attachments in emails. To improve workforce awareness, the internal security team may test the training of an organization's workforce with simulated phishing emails¹.

Proactive Prevention is the Best Defense

Prevention is the most effective defense against ransomware and it is critical to take precautions for protection. Infections can be devastating to an individual or organization, and recovery may be a difficult process requiring the services of a reputable data recovery specialist.

The U.S. Government (USG) recommends that users and administrators take the following preventive measures to protect their computer networks from falling victim to a ransomware infection:

Preventive Measures

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

¹ For additional information on Avoiding Social Engineering and Phishing Attacks, please see US-CERT Security Tip (ST04-014), available at: <https://www.us-cert.gov/ncas/tips/ST04-014>



- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

Business Continuity Considerations

- Back up data regularly. Verify the integrity of those backups and test the restoration process to ensure it is working.
- Conduct an annual penetration test and vulnerability assessment.
- Secure your backups. Ensure backups are not connected permanently to the computers and networks they are backing up. Examples are securing backups in the cloud or physically storing backups offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

What to Do If Infected with Ransomware

Should preventive measures fail, the USG recommends that organizations consider taking the following steps upon an infection with ransomware:

- **Isolate the infected computer immediately.** Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives.
- **Isolate or power-off affected devices that have not yet been completely corrupted.** This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.



- **Immediately secure backup data or systems by taking them offline.** Ensure backups are free of malware.
- **Contact law enforcement immediately.** We strongly encourage you to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance.
- **If available, collect and secure partial portions of the ransomed data that might exist.**
- **If possible, change all online account passwords and network passwords after removing the system from the network.** Furthermore, change all system passwords once the malware is removed from the system.
- **Delete Registry values and files to stop the program from loading.**

Implement your security incident response and business continuity plan. Ideally, organizations will ensure they have appropriate backups, so their response to an attack will simply be to restore the data from a known clean backup. Having a data backup can eliminate the need to pay a ransom to recover data.

There are serious risks to consider before paying the ransom. USG does not encourage paying a ransom to criminal actors. However, after systems have been compromised, whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees, and customers. Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting systems from backup. Ransomware victims may also wish to consider the following factors:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom.
- Some victims who paid the demand were targeted again by cyber actors.
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

How Law Enforcement Can Help

Any entity infected with ransomware should contact law enforcement immediately. Law enforcement may be able to use legal authorities and tools that are unavailable to most organizations. Law enforcement can enlist the assistance of international law enforcement partners to locate the stolen or encrypted data or identify the perpetrator. These tools and relationships can greatly increase the odds of successfully apprehending the criminal, thereby preventing future losses.

Federal law enforcement places a priority on conducting cyber investigations in a manner that causes minor disruption to a victim entity's normal operations and seeks to work cooperatively and discreetly with that entity. Federal law enforcement uses investigative measures that avoid unnecessary downtime or displacement of a company's employees. Federal law enforcement closely coordinates its activities with the affected organization to avoid unwarranted disclosure of information.

As an affected entity recovers from a cybersecurity incident, the entity should initiate measures to prevent similar incidents. Law enforcement agencies and the Department of Homeland Security's National Cybersecurity and Communications Integration Center can assist organizations in implementing countermeasures and provide information and best practices for avoiding similar incidents in the future. Additionally, the affected organization should conduct a post-incident review of their response to the incident and assess the strengths and weaknesses of its incident response plan.

Ransomware Variants²

Ransomware is a growing criminal activity involving numerous variants. Since 2012 when police locker ransomware variants first emerged, ransomware variants have become more sophisticated and destructive. Some variants encrypt not just the files on the infected device, but also the contents of shared or networked drives, externally attached storage media devices, and cloud storage services that are mapped to infected computers. These variants are considered destructive because they encrypt users' and organizations' files, and render those files useless until a ransom is paid.

Recent federal investigations by the FBI reveal that ransomware authors continue to improve ransomware code by using anonymizing services like "Tor"³ for end-to-end communication to infected systems and Bitcoin virtual currency to collect ransom payments. Currently, the top five ransomware variants targeting U.S. companies and individuals are CryptoWall, CTB-Locker, TeslaCrypt, MSIL/Samas, and Locky. New ransomware variants are continually emerging.

CryptoWall

CryptoWall and its variants have been actively used to target U.S. victims since April 2014. CryptoWall was the first ransomware variant that only accepted ransom payments in Bitcoin. The ransom amounts associated with CryptoWall are typically between \$200 and \$10,000. Following the takedown of the CryptoLocker botnet, CryptoWall has become the most successful ransomware variant with victims all over the world. Between April 2014 and June

² For more information on Ransomware variants and other resources, visit <https://www.us-cert.gov/ncas/alerts/TA16-091A>

³ Tor is free software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than 7,000 relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. (The name derives from the original software project name, *The Onion Router*.)

2015, IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over \$18 million.⁴ CryptoWall is primarily spread via spam email but also infects victims through drive-by downloads⁵ and malvertising⁶.

CTB-Locker

CTB-Locker emerged in June 2014 and is one of the first ransomware variants to use Tor for its C2 infrastructure. CTB-Locker uses Tor exclusively for its C2 servers and only connects to the C2 after encrypting victims' files. Additionally, unlike other ransomware variants that utilize the Tor network for some communication, the Tor components are embedded in the CTB-Locker malware, making it more efficient and harder to detect. CTB-Locker is spread through drive-by downloads and spam emails.

TeslaCrypt

TeslaCrypt emerged in February 2015, initially targeting the video game community by encrypting gaming files. These files were targeted in addition to the files typically targeted by ransomware (documents, images, and database files). Once the data was encrypted, TeslaCrypt attempted to delete all Shadow Volume Copies and system restore points to prevent file recovery. TeslaCrypt was distributed through the Angler, Sweet Orange, and Nuclear exploit kits.

MSIL or Samas (SAMSAM)

MSIL or Samas (SAMSAM) was used to compromise the networks of multiple U.S. victims, including 2016 attacks on healthcare facilities that were running outdated versions of the JBoss content management application. SAMSAM exploits vulnerable Java-based Web servers. SAMSAM uses open-source tools to identify and compile a list of hosts reporting to the victim's active directory. The actors then use psexec.exe to distribute the malware to each host on the network and encrypt most of the files on the system. The actors charge varying amounts in Bitcoin to provide the decryption keys to the victim.

Locky

In early 2016, a destructive ransomware variant, Locky, was observed infecting computers belonging to businesses globally, including those in the United States, New Zealand, Australia, Germany and the United Kingdom. Locky propagates through spam emails that include malicious Microsoft Office documents or compressed attachments (e.g., .rar, .zip) that were previously associated with banking Trojans such as Dridex and Pony. The malicious attachments contain macros or JavaScript files to download the Locky files. Recently, this ransomware has also been distributed using the Nuclear Exploit Kit.

⁴ This number includes additional costs incurred by the victim. Expenses may be associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and the purchase of credit monitoring services for employees or customers.

⁵ Drive by download" is the transfer of malicious software to the victim's computer without the knowledge of or any action by the victim.

⁶ "Malvertising," is the use of malicious ads on legitimate websites. These malicious ads contain code that will infect a user's computer without any action from the user (i.e., the user does not have to click on the ad to become infected).



Links to Other Types of Malware

Systems infected with ransomware are also often infected with other malware. In the case of CryptoLocker, a user typically was infected by opening a malicious attachment from an email. This malicious attachment contained Upatre, a downloader, which infected the user with GameOver Zeus. GameOver Zeus was a variant of the Zeus Trojan used to steal banking information and other types of data. After a system became infected with GameOver Zeus, Upatre would also download CryptoLocker. Finally, CryptoLocker encrypted files on the infected system and demanded a ransom payment.

The disruption operation against the GameOver Zeus botnet also affected CryptoLocker, demonstrating the close ties between ransomware and other types of malware. In June 2014, an international law enforcement operation successfully weakened the infrastructure of both GameOverZeus and CryptoLocker.

Federal Government Resources

Reporting

Federal Bureau of Investigation

Cyber Task Forces

www.fbi.gov/contact-us/field

Internet Crime Complaint Center

www.ic3.gov

United States Secret Service

Electronic Crimes Task Force

www.secretservice.gov/investigation/#field

Local Field Offices

www.secretservice.gov/contact/

Mitigation

Department of Homeland Security

United States Computer Emergency Readiness Team (US-CERT)

www.us-cert.gov

NIST Cybersecurity Framework:

<http://www.nist.gov/cyberframework/>

NSA/IAD Top 10 Information Assurance Mitigations Strategies:

<https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm>

Sen. John McCain Holds A Hearing On Foreign Cyber .., sked FINAL

January 5, 2017 3:21PM ET

TRANSCRIPT

January 05, 2017

COMMITTEE HEARING

SEN. JOHN MCCAIN

CHAIRMAN

SENATE COMMITTEE ON ARMED SERVICES

WASHINGTON, D.C.

SEN. JOHN MCCAIN HOLDS A HEARING ON FOREIGN CYBER THREATS TO THE
UNITED STATES

1255 22nd Street N.W.

Washington, D.C. 20037

Copyright 2017 Roll Call, Inc.

All materials herein are protected by United States copyright law
and may not be reproduced, distributed, transmitted, displayed,
published or broadcast without the prior written permission of
Roll Call. You may not alter or remove any trademark,
copyright or other notice from copies of the content.

SENATE COMMITTEE ON ARMED SERVICES HOLDS A HEARING ON

FOREIGN CYBER THREATS TO THE UNITED STATES

JANUARY 5, 2017

SPEAKERS:

SEN. JOHN MCCAIN, R-ARIZ.

CHAIRMAN

SEN. JAMES M. INHOFE, R-OKLA.

SEN. JEFF SESSIONS, R-ALA.

SEN. ROGER WICKER, R-MISS.

SEN. LINDSEY GRAHAM, R-S.C.

SEN. DEB FISCHER, R-NEB.

SEN. TED CRUZ, R-TEXAS

SEN. MIKE LEE, R-UTAH

SEN. TOM COTTON, R-ARK.

SEN. MIKE ROUNDS, R-S.D.

SEN. JONI ERNST, R-IOWA

SEN. THOM TILLIS, R-N.C.

SEN. DAN SULLIVAN, R-ALASKA

SEN. BEN SASSE, R-NEB.

SEN. DAVID PERDUE, R-GA.

SEN. JACK REED, D-R.I.

RANKING MEMBER

SEN. BILL NELSON, D-FLA.

SEN. CLAIRE MCCASKILL, D-MO.

SEN. JOE MANCHIN III, D-W.VA.

SEN. JEANNE SHAHEEN, D-N.H.

SEN. KIRSTEN GILLIBRAND, D-N.Y.

SEN. RICHARD BLUMENTHAL, D-CONN.

SEN. JOE DONNELLY, D-IND.

SEN. MAZIE K. HIRONO, D-HAWAII

SEN. TIM KAINE, D-VA.

SEN. MARTIN HEINRICH, D-N.M.

SEN. ELIZABETH WARREN, D-MASS.

SEN. GARY PETERS, D-MICH.

SEN. ANGUS KING, I-MAINE

WITNESSES:

JAMES R. CLAPPER JR.,

DIRECTOR OF NATIONAL INTELLIGENCE

MARCEL LETTRE,

UNDERSECRETARY OF DEFENSE FOR INTELLIGENCE,

DEPARTMENT OF DEFENSE

ADMIRAL MICHAEL S. ROGERS (USN),
DIRECTOR,
NATIONAL SECURITY AGENCY,
COMMANDER,
U.S. CYBER COMMAND

MCCAIN: Well, good morning -- good morning.

Before we begin, I -- I want to welcome all our members back to the committee and extend a special welcome to the new members joining us. On the Republican side we're joined by Senator Perdue and Senator Sasse. On the Democratic side we are joined by Senator Warren and Senator Peters.

MCCAIN: It's a special privilege to serve on this committee, most of all because it affords us the opportunity to spend so much time in the company of heroes: the men and women who serve and sacrifice on our behalf every day.

I hope you will come to cherish your service on this committee as much as I have over the years and I look forward to working with each of you.

The committee meets this morning for the first in a series of hearings on cyber security to receive the testimony on foreign cyber threats to the United States. I'd like to welcome our witnesses this morning; James Clapper, director of National Intelligence. Marcel Lettre, undersecretary of defense for intelligence, and Admiral Mike Rogers, commander of U.S. cyber command, director of the National Security Agency and chief of the Central Security Service.

This hearing is about the range of cyber security challenges confronting our nation. Threats from countries like Russia, China, and North Korea and Iran as well as non-state actors from terrorist groups to transnational criminal organizations. In recent years, we've seen a growing series of cyber attacks by multiple actors, attacks that have targeted our citizens, businesses, military, and government.

But there's no escaping the fact that this committee meets today for the first time in this new Congress in the aftermath of an unprecedented attack on our democracy. At the president's direction, Director Clapper is leading a comprehensive review of Russian interference in our recent election with a goal of informing the American people as much as possible about what happened.

I am confident that Director Clapper will conduct this review with the same integrity and professionalism that has characterized his nearly half a century of government and military service. I'm equally confident in the dedicated members of our intelligence committee -- community. The goal of this review, as I understand it, is not to question the outcome of the presidential election, nor should it be.

As both President Obama and President-elect Trump have said, our nation must move forward. But we must do so with full knowledge of the fact. I trust Director Clapper will brief the Congress on his review when it is completed. This is not the time or place to preview its findings.

That said, we know a lot already. In October, our intelligence agencies concluded unanimously that, quote, "The government -- the Russian government directed compromises of e-mails from U.S. persons and institutions including from U.S. political organizations."

They also assessed that, quote, "Disclosures of alleged hacked e-mails were consistent with the methods and motivations of Russian-directed efforts and that these thefts and disclosures were intended to interfere with the U.S. election process." Since then, our intelligence community has released additional information concerning these Russian activities including a joint analysis report that provided technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services to attack the United States.

Every American should be alarmed by Russia's attacks on our nation. There is no national security interest more vital to the United States of America than the ability to hold free and fair elections without foreign interference. That's why Congress must set partisanship aside, follow the facts, and work together to devise comprehensive solutions to deter, defend against and when necessary, respond to foreign cyber attacks.

As we do, we must recognize that the recent Russian attacks are one part of a much bigger cyber -- cyber problem. Russian cyber attacks have targeted the White House, the joint staff, the State Department, our critical infrastructure. Chinese cyber attacks have reportedly targeted NSA, the Department of State and Commerce, congressional offices, military labs, the Naval War College, and U.S. businesses including major defense contractors.

Most recently, China compromised over 20 million background investigations at the Office of Personnel Management. Iran has used cyber tools in recent years to attack the U.S. Navy. U.S. partners in the Middle East, major financial institutions, and a dam just 25 miles north of New York City, and of course, North Korea was responsible for the massive cyber attack on Sony Pictures in 2014.

What seems clear is that our adversaries have reached a common conclusion that the reward for attacking America in cyberspace outweighs the risk. For years, cyber attacks on our nation have been met with indecision and inaction. Our nation has no policy and thus no strategy for cyber deterrence. This appearance of weakness has been provocative to our adversaries who have attacked us again and again with growing severity.

Unless we demonstrate that the cost of...

MCCAIN: Unless we demonstrate that the cost of attacking the United States outweigh the perceived benefits, these cyber attacks will only grow.

This is also true beyond the cyber domain. It should not surprise us that Vladimir Putin would think he could launch increasingly severe cyber attacks against our nation when he had paid little price for invading Ukraine, annexing Crimea, subverting democratic values and institutions across Europe and of course, helping Bashar Assad slaughter civilians in Syria for more than a year with impunity.

The same is true for China, Iran, North Korea and any other adversary that has recently felt embolden to challenge the world order. Put simply, we cannot achieve cyber deterrence without restoring the credibility of the U.S. deterrence more broadly.

To do so, we must first have a policy which means finally resolving the long list of basic cyber questions that we as a nation have yet to answer. What constitutes an act of war or aggression in cyber space that would merit a military response?

Be it by cyber, or other means? What is our theory of cyber deterrence and what is our strategy to implement it? Is our government organized appropriately to handle this threat? Or are we so stove piped that we cannot deal with it effectively?

Who is accountable for this problem? And do they have sufficient authorities to deliver results? Are we in the Congress, just as stove piped on cyber as the executive branch, such that our oversight actually reinforces problems rather than helping to resolve them?

Do we need to change how we are organized? This committee intends to hold a series of hearings in the months ahead, to explore these and other questions. And we look forward to hearing the candid views of our distinguished witnesses today, who have thought about and worked on these questions as much as anyone in our nation.

Senator Reed?

REED: Well, thank you very much, Mr. Chairman. I want to commend you for your leadership in promptly scheduling this meeting on foreign cyber threats.

I'd also like to welcome our witnesses; Director Clapper, Undersecretary Lettre and Admiral Rogers, thank you gentlemen for your service and your dedication.

While I understand that our witnesses will be discussing the cyber threats that many countries, including China and India, pose to our nation I would like to focus for a few minutes on the widely reported instances of Russian hacking and disinformation that raised concerns regarding the election of 2016.

In addition to stealing information from the Democratic National Committee and the Clinton campaign and cherry-picking what information it leaked to the media, the Russian government also created and spread fake news and conspiracies across the vast social media landscape.

At the very least, the effect of Russia's actions was to erode the faith of the American people and our democratic institutions. These and other cyber tools remain highly active and engaged in misinforming our political dialog, even today.

There is still much we do not know, but Russia's involvement in these intrusions does not appear to be in any doubt. Russia's best cyber operators are judged to be as allusive and hard to identify as any in the world.

In this case, however, detection and attribution were not so difficult, the implication being that Putin may have wanted us to know what he had done, seeking only a level of plausible deniability of support and official rejection of culpability.

These Russian cyber attacks should be judged within the larger context of Russia's rejection of the post-Cold War international order and aggressive actions against its neighbors.

Russian's current leaders and President Putin in particular, precede the democratic movements in the form of Soviet States, the west general support for human rights, press against the rule of law and democracy, as well as NATO and E.U. enlargement, as a threat to what they believe is Russia's sphere of influence.

Putin's Russia makes no secret to the fact that it determined -- it is determined to aggressively halt and counter what is characterizes as western encroachment on its vital interest. Invasion of Georgia, the annexation of Crimea, the aggression against Ukraine featuring sophisticated hybrid warfare techniques, a continuing of those military build-up despite a declining economic, saber-rattling in the Baltic's and Baltic Sea, the authoritarian on float against the press, NGOs and what remains of the Russia democratic opposition, the unwavering campaign for national sovereignty over the internet and the creation of an iron information curtain.

Like China's great firewall and its aggressive interference in western political processes all are one piece. Russia's efforts to undermine democracy at home and abroad and destabilize a country is on its border, it cannot be ignored or traded away in exchange for the appearance of comity.

REED: Furthermore, what Russia did to the United States in 2016, it is already doing -- has done rather, and continues to do in Europe. This challenge, the progress of democratic values since the end of the Cold War must not be tolerated.

Despite the indifference of some to this matter, our nation needs to know in detail what the intelligence community has concluded was an assault by senior officials on a foreign government on our electoral process. Our electoral process is the bedrock of our system of government, an effort to manipulate it, especially by a regime with values and interests so antithetical to our own, is a challenge to the nation's security which must be met with bipartisan and universal condemnation, consequences and correction.

I believe the most appropriate means in conducting inquiry is the creation of a special select committee in the Senate. Since this issue and the solutions to the problems have been exposed, spill across the judicial divides of the standing committees on armed services, intelligence, foreign relations, homeland security, and judiciary. Failing that, our committee must take on as much of this task as we can. I again, commend the chairman for his commitment to do so.

Therefore I am pleased and grateful that his efforts will be expended, the energy will be invested on the matters that are so critical to the American people.

I also want to applaud president Obama's initial steps, publicized last week to respond to Russia's hostile actions. General Clapper, Undersecretary Lettre, Admiral Rogers, we appreciate your urgent efforts to discover what happened and why and to make these facts known to the president, the president-elect, Congress and the American people. Although your investigation to report to President Obama is not yet public, we hope you'll be able to convey and explain what's been accomplished so far, including the steps already announced by the president.

In addition I am sure we'll have many questions about how we are organized in the cyber domain and what changes you have recommended going forward. Subjects that President Obama referenced in his signing statement of the national defense authorization act for fiscal year 2017. These are difficult issues, but they are vital importance to our nation, our security and our democracy.

Mr. Chairman, I look forward to working with you in a bipartisan manner to conduct a thorough and thoughtful inquiry, and to do more to address the cyber threats our nation's basis, more broadly by state and non-state actions. Thank you very much.

MCCAIN: Welcome the witnesses and Mr. Secretary we'll begin with you for any opening statements or comments you might have.

LETTRE: Thank you Chairman, Ranking Member Reed, members of the committee. I appreciate the opportunity to be here today.

I will shortly turn the microphone over to Director Clapper for some comments followed by Admiral Rodgers. As this is my last appearance before this committee before stepping down from eight years of Pentagon service in a few weeks. I want to thank...

MCCAIN: I'm sure that that is -- I'm sure you'll regret not having that opportunity again.

LETTRE: It will be nice to be skiing a little bit in February, that's for sure.

But having said that, since I am just a few weeks from stepping down, I do want to thank this committee for its partnership and I want to thank Director Clapper and Admiral Rodgers for the privilege of being able to serve together with them and the leadership of the U.S. intelligence community.

And to the men and women of the U.S. intelligence community, civilian and military, thousands of whom are deployed today around the world advancing U.S. interest and protecting America. I do admire your integrity, I admire your service. It has been an honor to serve with you over the last many years.

In the interest of time, I'll briefly note the Department of Defense's views on cyber in three core themes. First, the threats we must address, second, what we are doing to address them now and third, the difficult, but urgent work we know still lies ahead.

First, the threats.

As you know, the Department of Defense's leadership believes we confront no fewer than five immediate, but also distinct and evolving challenges across all operating domains. We are countering the prospect of Russian aggression and coercion, especially in Europe, something we unfortunately have had to energetically renew our

focus on in the last several years. We are also managing historic change in perhaps the most consequential region for America's future, the Asia- Pacific and watching the risks of China's destabilizing actions in the region.

LETTRE: We are checking Iranian aggression and malign influence across the Middle East. We are strengthening our deterrent and defense forces in the face of North Korea's continued nuclear and missile provocations, and we are countering terrorism with the aim of accelerating the lasting defeat of...

XXX Across the Middle East. We are strengthening our deterrent and defense forces in the face of North Korea's continued nuclear and missile provocations. And we are countering terrorism with the aim of accelerating the lasting defeat of ISIL and Al Qaida. These are what many in the Department of Defense have termed the four-plus-one; Four state-based challenges and an ongoing condition of battling terrorism.

As our joint statement for the record has detailed, each of these security challenges; China, Russia, Iran, North Korea, and global terrorist groups such as ISIL, presents a significant cyber threat dimension to the U.S. military. Cyber is an operating domain that is real, complex, dynamic, contested, and must be addressed.

Second, what we are doing about it. The Department of Defense has, for several years, pursued a comprehensive strategy for maintaining the necessary strategic dominance in this domain. Secretary of Defense Ash Carter has pressed for DOD to change, to adapt, and to innovate not only to meet today's challenges, but also to ensure that we effectively defend against cyber threats well into an uncertain future.

We have built and continue to build the means and methods that will strengthen our relative position against each of these dimensions of the cyber threat. The government's cyber policies reflected in presidential policy directives and executive orders provide guidance on the absolute necessity of a whole of government approach critical to protecting our nation.

The department has developed, refined, and published its cyber strategy which clearly lays out three key DOD cyber missions; defending DOD networks, providing cyber options for our military commanders and when called upon by our nation's leaders, defending the nation against cyber attacks of significant consequence. As the director and Admiral Rogers will note, since 2009, the department has matured Cyber

Command to ensure clear command responsibility and authority and growing capabilities essential to our unity of effort for cyber operations.

We also continue to mature our cyber mission forces which this fall achieved initial operating capability or IOC status. This force is providing military capability to execute our three missions in cyberspace. We're building new capabilities and new tools for the cyber mission force to use.

Third, what remains to be done. As much as we have done, we recognize there is much more to do. Let me mention just a couple of those most important tasks here.

First, we need to continue to develop and refine our national cyber policy framework which includes the evolution of all dimensions of our deterrence posture, the ability to deny the adversary its objectives, to impose costs and to ensure we have a resilient infrastructure to execute a multi-domain mission.

This refinement and evolution in our deterrent thinking and capability will further empower decision-making at net speed. Second, within the department, Cyber Command has matured and is doing more to protect the nation and support global operations than ever before and we need to continue, in fact accelerate, this maturation.

Accordingly, the secretary of Defense supports the elevation of Cyber Command to a unified combatant command and supports ending the dual-hat arrangement for the leadership of NSA and Cyber Command, in doing so through a deliberate conditions-based approach while continuing to leverage the shared capabilities and synergies.

And finally, we must redouble our efforts to deepen partnerships between government and the private sector and between the U.S. government and our allies. We must continue to seek help from American industry, the source of much of the world's greatest technology talent and innovating to find cyber defense solutions, build resiliency into our critical infrastructure systems, and strengthen our deterrence.

With our international allies and partners we must work together to promote stability in cyber space, universal recognition that existing international law applies in cyberspace, and the adoption of voluntary peacetime norms of responsible state behavior.

Mr. Chairman, thanks. I look forward to your questions. I'll now pass the baton to Director Clapper. Thank you.

MCCAIN: General Clapper?

CLAPPER: Chairman McCain, Ranking Member Reed, and distinguished members of the committee, first, thanks very much for your -- your opening statements.

Obviously we're here today to talk about cyber threats that face our nation and I will offer some brief valedictory recommendations and a few parting observations.

I certainly want to take note of and thank the members of the committee who are engaged on this issue and have spoken to it publicly. I know there is great interest in the issue of Russian interference in our electoral process based on the many classified briefings the intelligence community has already provided on this topic to the Congress.

Secretary of Homeland Security Jeh Johnson and I have issued statements about it. The Joint Analysis Report that you alluded to, publicly issued by the Department of Homeland Security and the Federal Bureau of Investigation, provided details on the tools and infrastructure used by the Russian intelligence services to compromise infrastructure associated with the election, as well as a range of U.S. government, political and private sector entities, as you described.

As you also noted, the president tasked the intelligence community to prepare a comprehensive report on Russian interference in our election. We plan to brief the Congress and release an unclassified version of this report to the public early next week, with due deference to the protection of highly sensitive and fragile sources and methods. But until then, we're really not prepared to discuss this beyond standing by our earlier statements. We are prepared to talk about other aspects of the Russian cyber threat.

We also see cyber threats challenging public trust and confidence in information, services, and institutions. Russia has clearly assumed an even more aggressive cyber posture by increasing cyber espionage operations, leaking data stolen from these operations, and targeting critical infrastructure systems. China continues to succeed in conducting cyber espionage against the U.S. government, our allies, and U.S. companies.

The intelligence community and security experts, however, have observed some reduction in cyber activity from China against U.S. companies since the bilateral September 2015 commitment to refrain from espionage for commercial gain. Iran and North Korea continue to improve their capabilities to launch disruptive or destructive cyber attacks to support their political objectives.

Non-state actors, notably terrorist groups, most especially including ISIL, also continue to use the internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by disciples, and coordinate operations.

So in this regard, I want to foot-stomp a few points that I've made here before. Rapidly advancing commercial encryption capabilities have profound effects on our ability to detect terrorists and their activities. We need to strengthen the partnership between government and industry, and find the right balance to enable the intelligence community and law enforcement both to operate, as well as to continue to respect the rights to privacy.

Cyber operations can also be a means to change, manipulate or falsify electronic data or information to compromise its integrity. Cyberspace can be an echo chamber in which information, ideas or beliefs, true or false, get amplified or reinforced through constant repetition. All these types of cyber operations have the power to chip away at public trust and confidence in our information services and institutions.

By way of some observations or recommendations, both the government and the private sector have done a lot to improve cybersecurity, and our collective security is better, but it's still not good enough. Our federal partners are stepping up their efforts with the private sector, but sharing of what they have remains uneven. I think the private sector needs to up its game on cybersecurity and not just wait for the government to provide perfect warning or a magic solution.

We need to influence international behavior in cyberspace. This means pursuing more global diplomatic efforts to promulgate norms of behavior in peacetime and to explore setting limits on cyber operations against certain targets. When something major happens in cyberspace, our automatic default policy position should not be exclusive to counter cyber with cyber. We should consider all instruments of national power.

In most cases to date, non-cyber tools have been more effective at changing our adversary's cyber behavior. When we do choose to act, we need to model the rules we want others to follow since our actions set precedents. We also need to be prepared for adversary retaliation which may not be as surgical, either due to the adversary's skill or their inherent difficulty in calibrating effect and impact of cyber tools. That's why using cyber to counter cyber attacks risks unintended consequences.

We currently cannot put a lot of stock, at least in my mind, in cyber deterrence. Unlike nuclear weapons, cyber capabilities are difficult to see and evaluate and are ephemeral. It is accordingly very hard to create the substance and psychology of deterrence, in my view.

We also have to take some steps now to invest in the future. We need to rebuild trusted working relationships with industry and the private sector on specific issues like encryption and the roles and responsibilities for government, users, and industry. I believe we need to separate NSA and Cyber Com. We should discontinue the temporary dual-hat arrangement which I helped design when I was undersecretary of defense for intelligence seven years ago. This isn't purely a military issue. I don't believe it is in NSA's or the I.C.'s long-term best interest to continue the dual-hat setup.

Third, we must hire, train and retain enough cyber talent and appropriately fuse cyber as a whole-of-I.C. workforce. Clearly, cyber will be a challenge for the U.S., the intelligence community and our national security for the foreseeable future, and we need to be prepared for that. Adversaries are pushing the envelope, since this is a tool that doesn't cost much, and sometimes is hard to attribute.

I certainly appreciate, as we all do, the committee's interest in this difficult and important challenge. I'll wrap up by saying, after 53 years in the intelligence business in one capacity or another, happily I've just got 15 days left. I'll miss being involved in the intelligence mission, and I will most certainly miss the talented and dedicated patriots who are in the United States intelligence community.

I'm very proud of the community professionals I've represented here for the last six-and-a-half years who don't get much public recognition and who like it that way. They've always supported me, and I'm confident they will do no less for my successor whoever that turns out to be.

So let me -- with that, let me stop and pass to Admiral Rogers.

MCCAIN: Thank you, General.

Admiral Rogers?

ROGERS: Chairman McCain, Ranking Member Reed, members of the committee, good morning and thank you for the opportunity to appear before the committee today on behalf of United States Cyber Command and the National Security Agency.

I'm honored to appear beside Director Clapper and Undersecretary Lettre, and I applaud them both for their many years of public service. It's been a true honor, gentlemen.

When we last met in September, I discussed the changing cyber threat environment. And today, I look forward to further discussing this complex issue. Of course, some aspects of what we do must remain classified to protect our nation's security. So today, I will limit my discussion to those in the public domain.

We have seen over the course of the last year how this cyber threat environment is constantly evolving. We have all come to take for granted the interconnectivity that is being built into every facet of our lives. It creates opportunities and vulnerabilities. Those who would seek to harm our fellow Americans and our nation utilize the same internet, the same communications devices, and the same social media platforms that we, our families, and our friends here and around the world use.

We must keep pace with such changes in order to provide policy-makers and our operational commanders the intelligence and cyber capabilities they need to keep us safe. That means understanding our adversaries to the best of our ability, and understanding what they mean to do and why.

We're watching sophisticated adversaries involved in criminal behavior, terrorism planning, malicious cyber activities, and even outright cyber attacks. While this is a global problem, we have also recently witnessed the use of these tactics here at home.

A statement for the record that we have provided jointly to this committee covers the threat picture worldwide. But I know this hearing today will inevitably focus on reports of interference in our recent elections. I echo Director Clapper in saying that we will await

the findings of the just-completed intelligence review ordered by the president and defer our comments on its specifics until after that review is shared with our leaders and congressional overseers.

I do want to add, however, that over this last year, NSA and Cyber Command have worked extensively with our broader government partners to detect and monitor Russian cyber activity. The hacking of organizations and systems belonging to our election process is of great concern and we'll continue to focus strongly on this activity.

ROGERS: For NSA's part, we focus on the foreign threat actor in foreign spaces, but we share our information as readily as possible with the rest of our partners in the Department of Defense, the intelligence community and federal law enforcement, as well as others within the U.S. government and the private sector.

As you know, Russian cyber groups have a history of aggressively hacking into other country's government, infrastructure and even election systems. As I've indicated, this will remain a top priority for NSA and U.S. Cyber Command.

In this changing threat environment, I'd like to take this opportunity to emphasize the importance of improving cyber security and working related issues across public and private sectors. We continue to engage with our partners around the world, on what is acceptable and unacceptable behavior in cyber space. And we clearly, are not where we want to be, nor where we need to be in this regard.

We continue to make investments and technologies and capabilities to improve detection of malicious cyber activities and make it more difficult for malicious cyber actors intending to do us harm. Combating cyber threats take more than technology. It takes talented, motivated people. And we are investing more than ever in the recruitment and retention of a skilled work force that is knowledgeable, passionate and dedicated to protecting a nation for the safety of our citizens and of our friends and allies around the world.

Innovation is one of the key tenants of NSA and Cyber Command and we need to invigorate the cyber work force that think creatively about challenges that do not ascribe to traditional understandings of borders and boundaries. This remains a key driver and a key challenge, as we look to the future.

Cyber command is well along in building our cyber mission force, deploying teams to defend the vital networks that support DOD operations, to support combatant commanders in their missions worldwide and to bolster DOD's capacities and capabilities to defend the nation against cyber attacks of significance consequence.

The organizations I lead, U.S. Cyber Command and the National Security Agency, have provided intelligence, expert advice and tailored options to the nation's decision makers in response to recent events. Much of their activities can only be discussed in classified channels, but I must say, I'm proud of what both organizations have accomplished and will accomplish, even as we acknowledge we have to do more.

I look forward to your questions and finally, on one personal note. I apologize to all of you, I have an ongoing back issue. And if I have to stand up in the course of this time period, please don't take that as a sign of disrespect in any way. I guess I'm just getting older.

That's all I have for you, sir.

MCCAIN: I know how you feel.

(LAUGHTER)

Director, I just have to -- General Clapper, I just have to mention, the name Mr. Assange has popped up. And I believe that he is the one who's responsible for publishing names of individuals that work for us that put their lives in direct danger, is that correct?

CLAPPER: Yes, he has.

MCCAIN: And do you think that there's any credibility we should attach to this individual, given his record of -- of...

CLAPPER: Not in my view.

MCCAIN: Not in your view.

Admiral Rogers?

ROGERS: I second those comments.

MCCAIN: Thank you.

For the record, on October 7th, the Homeland Security and Office of Director of National Intelligence, their assessment was that U.S. intelligence community is confident that the Russian government directed their recent compromise of e-mails from U.S. persons and institutions, including from the U.S. political organizations.

It goes on to say, these thefts and disclosures are intended to interfere with the U.S. election process, quote, "Such activity is not new to Moscow, Russians have used similar tactics and techniques across Europe and Eurasia."

Quote, "Based on the scope and sensitivity of these efforts, that not -- that only Russia's senior most officials could have authorized these activities."

General Clapper, do you --- those are still operable and correct statements?

CLAPPER: Yes, Chairman McCain, they are. As I indicated in my statement, we stand actually more resolutely on the strength of that statement that we made on the 7th of October.

MCCAIN: I thank you. And so really, what we're talking about, is if they succeeded in changing the results of an election of which none of us believe they were, that would have to constitute an attack on the United States of America because of the effects, if they had succeeded, would you agree with that?

CLAPPER: First, we cannot say -- they did not change any vote tallies or -- or anything of that sort.

MCCAIN: Yeah, I'm just talking about...

(CROSSTALK)

CLAPPER: And we have no -- we have no way of gauging the impact that -- certainly the intelligence community can't gauge the -- the impact it had on the choices the electorate made. There's no way for us to gauge that.

Whether or not that constitutes an act of war I think is a very heavy policy call that I don't believe the intelligence community should make. But it's certainly -- would carry in my view great gravity.

MCCAIN: Thank you.

Admiral Rogers, have you seen this problem in your position getting worse or better? In other words, it's my information that their techniques have improved, their capability's improved, the degree of success has -- has improved.

Is that -- is your -- is that your assessment?

ROGERS: So, I -- I -- I have publicly said before that the Russians are -- are a feared competitor in cyber. If you look broadly beyond the Russians to cyber at large, the level of capability of nation states and actors around the world continues to increase. I can't think of a single significant actor out there who is either decreasing their level of investment, getting worse in their trade craft or capability, or in any way backing away from significant investments in cyber.

MCCAIN: And with all due respect, you Mr. Secretary, I have not seen a policy -- in other words, I don't think any of our intelligence people know what to do if there is an attack besides report it. I don't think that any of our people know if they see an attack coming what specific actions should be taken.

Maybe I'm missing something, but I've asked time after time, what do you do in the case of an attack? And there's not been an answer. There's not been an answer.

And I -- I -- I believe that unless we have specific instructions to these wonderful men and women who are doing all of this work, then we're going to be bystanders and observers. You know, I'm glad to hear you respond to that.

LETTRE: Mr. Chairman, you're right that we have a lot more work to do to put the right deterrence and response framework in place on cyber. This is somewhat of a new domain of operations and in some cases warfare.

And in -- in -- in my personal opinion, the next administration would -- would be well served to focus very early on -- on those questions of -- of continuing to develop our --

our overarching policy, a comprehensive approach, and a -- a increasingly robust and refined deterrence framework.

MCCAIN: Thank you.

Finally, Director and Admiral, would it make your job easier if you didn't have to report to seven different committees?

(LAUGHTER)

CLAPPER: Chairman McCain, my hands have been slapped before when I ventured into the delicate area of congressional jurisdictions. So for...

(LAUGHTER)

MCCAIN: Even in the last...

CLAPPER: ... the remaining 15 days that I'm in office, I don't think I'm going to speak to that. Afterwards, I might be different.

MCCAIN: Well, we look forward to calling you back.

(LAUGHTER)

Admiral Rogers...

ROGERS: Should I second the comments of the Director of National Intelligence?

MCCAIN: But it -- it -- it does make it difficult, doesn't it? With the -- it's not exactly stove piping, but overlapping jurisdictions I think makes your job a little harder, doesn't it? I mean in all candor, Admiral.

ROGERS: I mean, the way I would phrase it is I think clearly an integrated approach is a key -- is a key component of our ability to move ahead here. I -- I would say that in the government, in the private sector, there -- there's no particular one slice where that's not applicable.

MCCAIN: Thank you.

Senator Reed?

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

And General Clapper, you responded to the Chairman that in October you and the Director of Homeland Security concluded that the Russian government intervened in the election and Admiral Rogers also seconded that view. That is also today the view for the record of the FBI and the Central Intelligence Agency -- in fact, all the intelligence communities, is that correct?

ROGERS: Yes, the forthcoming report is done essentially by those three agencies, CIA, FBI, and NSA.

REED: And the same conclusion with respect to the involvement of high-level Russian authorities is -- is shared by the -- all of these agencies?

ROGERS: Yes.

REED: The -- the chairman just noticed the -- the legislative compartmentalization. Does that reflect also in terms of operations, in terms of -- for example, Admiral Rogers, if you, through NSA or through your sources detect a -- something that is obviously a -- a disruption, something that is patently wrong, you can communicate to the FBI or law enforcement, but there's no mechanism to make things happen administratively, is that fair?

ROGERS: There's certainly process and, in fact, there have been several instances that I can think of in the last 18 months where we have run through that same scenario. Intelligence as it does in many other areas -- other domains, will detect incoming activity of concern. We -- NSA, will partner with FBI, the Department of Homeland Security, U.S. Cyber Command, to ensure the broader government -- the Department of Defense and FBI and its relationship with the private sector.

The biggest frustration to me is speed, speed, speed. We have got to get faster, we've got to be more agile. And, so for me at least within my span of control, I'm constantly asking the team, what can we do to be faster and more agile? How do we organize ourselves, what's the construct that makes the most sense? We can't be bound by history and tradition here, so to speak. We have to be willing to look at alternatives.

REED: Thank you.

General Clapper, one of the aspects of this Russian hacking was not just disseminating information that they had exploited from computers, but also the allegations of fake news sites, fake news stories that were propagated. Is that accurate or is that one aspect of this problem?

CLAPPER: Yes, without getting too far in front of the headlights of our roll out next week to the Congress. That was -- this was a multifaceted campaign, so the hacking was only one part of it. And, it also entailed, you know, classical propaganda, disinformation, fake news.

REED: Does that continue?

CLAPPER: Yes.

REED: Do the Russians particularly are very astute at covering up their tracks. It appears that they weren't quite as a diligent or -- let me ask a question. Do you believe that they made little attempts to cover up as a way to make a point politically?

CLAPPER: Again, without preempting the report, that's classical trade craft that the Russians have long, long used to particularly -- propagating so called disinformation is they will often try to hide the source of that or mask it to -- to deliberately mask the source.

REED: I -- let me just ask one more time. In this situation though, was there attempts to mask their involvement very elaborate and very, very sophisticated, or was just enough to have plausible deniability?

CLAPPER: Sir, I'd rather not get into that. That kind of edges into the sources and methods I run (ph) and I'd rather not speak to that publicly.

REED: Fair enough. This -- these activities are ongoing now in Europe as Europe prepares for elections. Is that a fair assumption?

CLAPPER: It is.

REED: Thank you. Yesterday the Wall Street Journal indicated that the President-elect is considering changes to the intelligence community. Have you at all as the expert in this field, been engaged in any of these discussions, deliberations, advice?

CLAPPER: No, we have not.

REED: Thank you, Mr. Chairman.

MCCAIN: (OFF-MIKE)

INHOFE: Thank you, Mr. Chairman.

The -- I heard this morning that a lot of the news media was characterized in this as a hearing on Russian hacking and actually it's on foreign cyber threats to the United States. I would like to cover a couple of the other ones.

First of all, I received something this morning, Director Clapper that I was very glad to read.

I've often said that the threats we're facing today are greater. I look wistfully back at the days of the Cold War. You're statement that I -- that was in print this morning said, sometimes all of this makes me long for the Cold War when world has essentially had two large mutually exclusive and so forth.

INHOFE: You know I think it's important that we talk about this because the general public is not aware that the nature of the threats that are out there that have not been out there before.

Admiral, on -- no Director Clapper, we've had a lot of -- and most damaging cyber attacks perpetrated against American people when the Chairman gave his opening statement, he singled out three or four of them, one of them was the OPM incident, that was 2014 and '15, Office of Personnel Management, it was a breach and threat to personnel -- personal information, birth dates, home addresses, social security numbers of over 22 million individuals.

I'd like to ask you, what action was taken after that and what kind of effect that might have had on the behavior of the Chinese?

CLAPPER: Well, the major action that we took, of course, was remediation in terms of advising people of what the potential risks were and, of course, there was a lot of work done, NSA was deeply involved in this, in enhancing or improving the cybersecurity posture of OPM and Admiral Rogers might speak to that.

I would say that this was espionage. It was not an attack per say; and of course, I was a bit reticent about, you know, people that live in glass houses shouldn't throw publicly too many rocks. So there isn't I think a difference between, you know, an act of espionage, which we conduct, as well, and other nations do, versus an attack.

Mike, you want to comment?

ROGERS: Just as a broader point, I think the OPM issue highlights that massive data concentrations increasingly have value all of their own.

What do I mean by that? I can remember 10 years ago, earlier in my time in cyber thinking to myself, large data bases like OPM are so large, the ability of an intruder and external actor to actually access, fully extract and bore their way through millions upon millions of millions of records would be difficult.

But with the power of big data analytics, large data concentrations now become increasingly attractive targets because the ability to mine that data for insights, which is what we think drove this action in the first place, becomes more and more easily done.

INHOFE: OK, I appreciate that very much. In your joint statement -- and by the way I like the idea of joint statements; it makes our questioning a lot easier.

You talk about the -- you end up stating through one of your paragraphs, in short, cyber threat cannot be eliminated, rather cyber threat must be managed. And it's interesting that in the Edison Electric Institute, it's a publication I think that came in this morning, they say exactly the same thing.

It seems to be one of the rare cases where we have government and industry working together. Their statement was that electric power industry recognizes it cannot protect all assets from all threats and instead must manage risk. Now they go on to describe the working together with government and they say the industry security strategies

constantly evolve and are closely coordinated with the federal government through a partnership called the Electricity Subsector Coordinating Council, the SCC.

Is that something you can comment? Is that -- are we looking at getting some success out of that?

CLAPPER: I think it's emblematic of a lot of work that the intelligence community has done, Department of Homeland Security, in engaging with each of the, I think 16 key infrastructure sectors in this country. And providing what we have embarked on as providing them tailored to each one of those sectors intelligence estimates of what the threats and vulnerabilities are in order to help them take measures to enhance our cybersecurity.

I think the major point there is if there is any connection whatsoever with the internet there is an inherent security vulnerability, and we have to manage that, the risk that is generated accordingly with full knowledge of that fact. If there's an internet connections, there's always going to be a vulnerability.

CLAPPER: Mike?

ROGERS: I would echo that.

I think part of our challenge is, our defensive strategy must be two-pronged, we have to spend time making it difficult for people to gain access, but we must acknowledge that despite our best efforts, there is a probability that they are still going to get in. So what do you do?

As a guy who defends networks on the Cyber Command side, I would tell you is a whole different thought process, methodology, prioritization and risk approach in dealing with someone who's already in your network versus trying to keep them out in the first place and we have to be able to do both.

INHOFE: All right, I appreciate that, my time has expired. I have one last question, just for the record you can not answer at this time. But a year ago, it was a year and two months ago I think it was Admiral Rogers, you made a statement before this committee that we -- quote, "We have peer competitors in cyber space and some of them have

already hinted that they hold the power to cripple our infrastructure and set back our standard of living if they choose."

I'd like for the record, if you could just kind of outline which of our peer competitors might be the closest to choosing...

(CROSSTALK)

ROGERS: ... as I have publicly said before, the Russians are the -- the peer competitors to us. But I look at other nations, you look at China for example and the level of capability and investment they're making on watching their abilities rise significantly.

Iran, North Korea, currently at a moderate level. But clearly, the level investment, the capability we're seeing and their willingness to employ cyber in some very aggressive ways that would be way beyond our normal risk...

(CROSSTALK)

MCCAIN: (OFF-MIKE)

NELSON: I think it is the general assumption that you all have said that our systems can be invaded, that has the American people, we as policy makers concerned. But the average American concern that there is no privacy anymore.

General, do you think in the report next week that you all will ascribe a motivation to Putin for election attempt?

CLAPPER: Yes, we will ascribe a motivation. I'd rather not, again, preempt the report.

NELSON: Understood. Well, then, will you discuss after the report, what is sufficient in the future to impose enough cost to make them stop this kind of activity?

CLAPPER: No, we won't. We -- if we're going to speak to that that would be separate from the report. What the report will include, per the president's tasking, was a section contributed by the Department of Homeland Security and NIST, I believe, on best practices for defending.

But it does not speak to that which is really out of our lane. That's a -- that's a policy call.

NELSON: So we're now talking about deterrence. And as one of you said in your testimony, it's not like a nuclear standoff of mutually assured destruction, because we don't have a particular deterrence now. Would you discuss that?

CLAPPER: What I was -- the point I was trying to make is that in the case of a nuclear deterrence, there are instruments you can see, feel, touch, measure. Weaponry, we've had demonstration, long time ago, of the impact of nuclear weaponry.

And that is what creates both the physical substance of deterrence, as well as the psychology. And the problem with the cyber domain, it's not -- it is not -- it doesn't have those physical dimensions that you can measure, see, feel, and touch as we do with nuclear deterrence.

NELSON: So let me give you an example. Help us understand, had the supposed invasion into the Vermont utility been, in fact, an invasion by a foreign power. And ascribed to that was shutting it down, if that had been the case, what would be some of the options that we would do?

CLAPPER: Well, then -- again, this would be -- as I understand it, by the way, it was not, but had it been from say malware planted by foreign power, I think that something would be a very situational dependent as what to do about it. As I indicated in my remarks, perhaps a cyber reaction to a cyber act, it may not be the best course of action.

Some other form of national power, sanctions is what we have traditionally used. And as I also indicated the problem, at least for me, is -- and I'll ask others to speak if they want to, is not knowing if -- you do retaliate in a cyber context, not knowing exactly what counter retaliation you'll get back.

Now we go through all kinds of exquisite thought processes on deciding how to react where we try to be very surgical, very precise, try to gauge what the second order or unintended consequences might be. I don't think others are similarly disposed to consider such precision and such exactness when they respond. So there's always that issue of counter retaliation, ergo, my brief mentioned that it's, in my view, best to consider all instruments of national power.

NELSON: And I think that's what's concerning us. Could we -- the United States, do we have the ability that we can make it so tough on North Korea, with a cyber attack, that it would deter them from some of their strange behavior?

CLAPPER: Not necessarily via a direct cyber reaction, given the difficulty of gaining access to their cyber networks.

MCCAIN: (OFF-MIKE)

WICKER: Thanks you.

Director Clapper, you're pretty far along on the report that will be released next week, obviously. How far along are you, and what do you lack and -- and -- and how will this released? Will it be in a classified format, will you -- will you have a deep willing to testify in an open hearing like this? Or would we need to go down to SCIF to hear this?

CLAPPER: What's -- what's planned is a series of briefings. In the Congress, I think I have four more hearings to do. First with our oversight committees which will be closed hearings I believe. And then they'll be...

WICKER: And when will that be?

CLAPPER: And all House, all Senate hearings, I believe next week as we roll out a version of the report early...

WICKER: So that will -- those will...

(CROSSTALK)

CLAPPER: ... to be followed by an unclassified version.

WICKER: I see. So the -- the public will not hear sources and methods, but they'll -- you think it will be fairly convincing without going beyond what...

CLAPPER: I assure you we intend -- I intend to be -- to push the envelope as much as I can on -- particularly on the unclassified version, because I think the public should know as much about this as possible. This is why I felt very strongly about the statement we made in October. And so we'll be as forthcoming as we can, but there are some

sensitive and fragile sources and methods here, which is one reason why we're reticent to talk about it in this setting.

WICKER: Right, and you've said that, and I expect you will be challenged with some very talented questioners up and down the dais here today on that.

I would have to support what Senator Nelson has said. As regrettable and reprehensible as the hacking of political parties is, I do think Senator Nelson has -- has touched on, really, the larger issue, which really is the subject matter of this hearing and that's what the -- what the real threats are.

WICKER: And it concerns me that -- that -- that we really don't know what the deterrents ought to be, and I wonder, at what -- at what level our conversations taking place within the administration or within the intelligence community, about what is appropriate in terms of a response? You mentioned cyber -- countering cyber with cyber is not necessarily the number one solution. Secretary Lettre mentioned that we should impose costs and perhaps after you answer I can ask him to expound on that also.

CLAPPER: Well, we have had many discussions in the White House situation room that deputies committee, principals (ph) committee and NSE meetings about what to do when we have these attacks. I think this -- the Sony attack by the North Koreans is a case in point.

And there you get into the complexities of -- do you launch a counter cyber -- a counter cyber attack and your -- want to be careful here, but you have to use some other nations infrastructure in order to mount that attack. And, that gets into as I have learned complex legal issues involving international law. And, so the judgment was to impose some other cost other than a direct cyber retaliation.

WICKER: Did you recommend that the president's sanctions was -- were his actions in response to the Russian hacking part of your recommendation or did that come from someone else?

CLAPPER: Oh that was -- well, without going into internal decision making, I think that was a, you know, it was a consensus interagency view.

WICKER: Secretary Lettre, what about -- what about imposing costs? What did -- what did you mean by that?

LETTRE: Well, as part of an approach that -- to deterrence that takes each case as it comes up, case by case. We need to look at ways to respond -- first deter and then respond to attacks at a time and a place of our choosing that favors advantages that we have as we use all of the instruments available.

So we look to deny objectives and then impose costs as you indicated Senator. Imposing costs really can come from things like -- were announced last week with the sanctions that were applied in the case of the Russian hacking situation. But they can go more broadly than that.

From the militaries perspective, we're concerned, not just about Russia's cyber hacking, but also about a range of aggressive actions by Russia across multiple regions in the globe. And, so we look to impose costs on Russia by a range of measures across multiple regions in partnership with our allies, through NATO, where we can -- to push back on Russian actions and deter future aggressive actions. So that's a bit of what we mean by imposing costs here.

WICKER: Thank you.

MCCAIN: It seems that every attack is handled on a case by case basis and that's not a strategy.

Senator McCaskill.

MCCASKILL: Thank you.

I know this is probably confuse you a little bit General Clapper, but review again how long you have been working in intelligence?

CLAPPER: I started in 1963, so.

MCCASKILL: And, you enlisted in '63 correct?

CLAPPER: No I enlisted in the Marine Corp in 1961.

MCCASKILL: And, then transferred to the Air Force?

CLAPPER: Right.

MCCASKILL: And you flew combat -- support for combat missions in Vietnam?

CLAPPER: I did two tours in Southeast Asia, one in Vietnam in 1965 and '66. And, then I was stationed in Thailand flying reconnaissance missions over Laos and Cambodia in 1970 and '71.

MCCASKILL: And, would you say that your experience in the military and especially your service for the government has always been for either political party and apolitical in terms of your mission and your job?

CLAPPER: Absolutely. I have served -- I toiled in the trenches in intelligence for every president since President Kennedy. I have served as a political appointee in both Republican and Democratic administrations.

MCCASKILL: Would say that ...

CLAPPER: So I am -- I am apolitical.

MCCASKILL: And by the way -- there are -- without getting into classified information, there are thousands of men and women who are working in the intelligence community right now, General Clapper, correct?

CLAPPER: Absolutely.

MCCASKILL: And, would you say that their experience in many instances mirrors yours? In terms of military experience, many of them being either active military or retired military?

CLAPPER: Yes, a large part of the intelligence community work force, are military. And of course there are many former military, either those who completed full careers or those who served enlistments or briefly and then came to the intelligence community as civilians.

MCCASKILL: Would you think it any less important that we maintain the intelligence community as foundational apolitical block of our country in terms of its protection?

CLAPPER: I -- I could not feel stronger about exactly that. I think it's hugely important that the intelligence community conduct itself and be seen as independent, providing unvarnished, untainted, objective, accurate and timely relevant intelligence support to all policy makers, commanders, diplomats, et cetera.

MCCASKILL: Do, in fact, the intelligence community -- members of the intelligence community engage in life-threatening and very dangerous missions every day particularly as it relates to the war on terror?

CLAPPER: You only need to walk into the lobby CIA and look at the stars on the wall or the front lobby of NSA and a number of intelligence people that have paid the ultimate price in the service of their country.

MCCASKILL: So let's talk about who benefits from a president- elect trashing the intelligence community. Who benefits from that Director Clapper, the American people? Them losing confidence in the intelligence community and the work of the intelligence community. Who -- who actually is the benefactor of someone who is about to become commander-in-chief trashing the intelligence community?

CLAPPER: I think there is an important distinction here between healthy skepticism, which policy makers -- to include policy maker number one -- should always have for intelligence, but I think there's a difference between skepticism and disparagement.

MCCASKILL: And I assume that the biggest benefactors of the American people having less confidence in the intelligence community are, in fact, the actors you have named today; Iran, North Korea, China, Russia and ISIS.

CLAPPER: The intelligence community is not perfect. We are an organization of human beings and we're prone, sometimes, to make errors. I don't think the intelligence community gets the credit it's due for what it does day in and day out to keep this nation safe and secure and a number of plots to -- just one example, terrorist plots that have been thwarted. Both those focused on this country and other countries.

MCCASKILL: I just -- I wanna thank the Chairman and I want to thank Senator Graham and others. There have been others I can count on maybe a little bit more than one hand who have stood up in a non- political way to defend the intelligence community over the last few weeks.

The notion that the elected -- soon elected leader of this country would put Julian Assange on a pedestal compared to the men and women of the intelligence community and the military that is so deeply embedded in the intelligence community, I think it should bring about a hue and cry no matter whether you're a Republican or a Democrat, there should be howls.

And mark my word, if the roles were reversed, there would be howls from the Republican side of the aisle. Thank you, Mr. Chairman.

MCCAIN: Thank you for that non-partisan comment.

(LAUGHTER)

Director Clapper, how would you describe Mr. Assange?

CLAPPER: How would I describe...

MCCAIN: Mr. Assange?

CLAPPER: Well, he's holed up in the Ecuadoran embassy in London because he's under indictment, I believe, by the Swedish government for a sexual crime. He has -- in the interest of -- ostensibly opened this in transparency. He exposed -- and his prior exposures put people at risk by his doing that.

So I don't think those with the intelligence community have a whole lot of respect for him.

MCCAIN: Admiral?

ROGERS: I would add to those comments.

MCCAIN: Thank you.

Senator Fischer?

FISCHER: Thank you, Mr. Chairman.

And thank you, gentlemen, for being here today and I do thank you for your service.

FISCHER: Gentlemen, as you all know, about a year ago Congress passed the Cybersecurity Information Sharing Act. And Director Clapper, could you comment on what steps have been taken to implement the act, in particular to provide cyber threat information in the possession of the federal government to non-government entities?

CLAPPER: There's been a lot of work done and this is principally through both the FBI and Department of Homeland Security to share more broadly with the private sector. This is -- prior to the enactment of this act, I think that this has been a theme that we have all worked -- worked hard, certainly one of the reasons for the creation of the Office of Director of National Intelligence was to assume a domestic role as well and to promote sharing as much as we can.

I think a lot of improvement has been made as I look back over the last 15 years, but there is more work to do. So we have done a lot of work with -- for example fusion centers, the 76 or so fusion centers that exist throughout the country to convey more information to them.

I have a network of 12 domestic DNI reps, Director of National Intelligence representatives, which are FBI special agents in charge, and we work through them -- those instrumentalities on a regional basis to convey more information, particularly on cyber threats to the private -- to state local officials as well as the private sector.

FISCHER: Thank you sir.

And Admiral Rogers, what is your assessment of the current state of information sharing between the government and private sector, especially regarding cybersecurity threats. And more importantly, what is the appropriate level of expectation to have with respect to that information sharing?

ROGERS: So, in some ways I characterize it as uneven. Some sector relationships -- as you heard General Clapper talk about the 16 sectors within the critical infrastructure of our nation. Some sectors, the relationship is very mature, information tends to flow

very regularly. Other sectors it's not quite as mature. I think the positive side is with the legislation we now developed a frame work for how we do it.

I still am concerned on the government side -- I'll only speak for NSA and cyber command -- on the government side, I'm not entirely comfortable that the products that I am generating are optimized to achieve outcomes for our, you know, private counter parts. I'm always trying to mind our team. Our success needs to be defined by the (inaudible) not about what we think is the right format or the right things to share.

FISCHER: You think there's any additional legislation that's going to be required that -- I guess I'm asking, what do you need? Do you think there's proper authorities that are currently in place or do we need new legislation or do you -- do you guys just need to improve on your execution of it?

ROGERS: Probably all of the above, to be very honest. I look at -- what are the changes that we're gonna need collectively to create the workforce of the future? Does the current structure I work within a DOD and an intel framework, but I would argue this is kind of universal. It doesn't matter where you're working, when is the structure, what's the recruitment and the benefit process that we need to retain and attract a workforce?

I'm curious with a new administration coming in, their broad view of roles and responsibilities. Are they comfortable with the current structure? Will their view be that we need to fundamentally relook at something different? I'd be the first to acknowledge as I previously said this morning -- we have got to get faster. We have got to get faster.

FISCHER: You know you've talked about case by case and the ad hoc nature of the -- our policies when it comes to cyber space before this committee, many many times. And, that's been an issue that this committee and the ETC Subcommittee in particular has tried to address by requiring strategies so that we can deter these hostile actors and delegations of authority, a definition of what an act of war in cyber space is.

You know we can go on and on. The chairman just mentioned, we don't have a strategy. Some of us just don't feel there's -- there's a strategy that's laid out there.

FISCHER: When you talk about speed and dealing with cyber attacks, I assume you are just referring to our -- our agencies and -- and responding to attack that is directly upon us. Do you think there needs to be any kind of consensus building on the international

stage with our allies in order to increase speed or would that delay it even more trying to run this through -- through channels and trying to respond quickly?

Do we reach -- do we reach out to allies, or do we perform our first duty in protecting this country?

ROGERS: So we routinely do that now. You clearly have highlighted it's a bit of a double edged sword. But it goes to the point from my perspective; cyber just doesn't recognize many of these boundaries. And so when you're trying to deal with an incident, is this something that is truly totally domestic or has it originated from somewhere external derivation (ph)?

What kind of infrastructure did it pass through? There's a whole lot of complexity to this, so I -- I apologize. It's not a simple binary choice there, even as I acknowledge there are tradeoffs.

FISCHER: Thank you.

Thank you, Mr. Chair.

MCCAIN: (OFF-MIKE)

BLUMENTHAL: Thanks Mr. Chairman.

I want to join Senator McCaskill in expressing my appreciation for the service of our intelligence community and to you, Mr. Chairman, for your very strong and courageous statements in support of the work of this committee to give credit and credibility to that intelligence community and to your statements also about the importance of cyber warfare.

It's not the first time we've been here on this topic and you have been resolute and steadfast in seeking to elevate public awareness and public consciousness about the importance of cyber attacks on this country and the threat of cyber warfare. And I want to explore a little bit why these demeaning and dismissive comments about our intelligence community are so dangerous to our nation.

Is it not true, Mr. Clapper, that public support for robust responses to cyber attacks on our nation depends on the credibility of our intelligence community and dismissing the

conclusions -- very credible and significant conclusions about the Russian attack, undermines public support for actions that the president must take to deter and punish these kinds of actions?

CLAPPER: I do think that public trust and confidence in the intelligence community is -- is crucial. And both -- both in this country and I think the dependents that other countries -- other nations have, on the U.S. intelligence community. And I've received many expressions of concern from foreign counterparts about the, you know, the disparagement of the U.S. intelligence community, or I -- I should say what has been interpreted as disparagement of the intelligence community.

BLUMENTHAL: Well, there's no question about the disparagement. There's no question about the dismissing and demeaning of the intelligence community entirely unmerited, and would you agree in light of your saying, that you are even more resolute now in your conclusion about Russia involvement in this hacking, that comparing it to the judgment made about weapons of mass destruction in the Iraq situation is totally a red herring, totally wrong?

CLAPPER: I -- yes, I agree with that. I -- my fingerprints were on that national intelligence estimate, I was in the community then. That was 13 years ago. We have done many, many things to improve our processes, particularly with respect to national intelligence estimates, in order to prevent that from happening again. Whatever else you want to say about the intelligence community, it is a learning organization, and we do try to learn lessons.

It's a very difficult business and getting harder all the time. And there will be mistakes, but what we do try to do, as we did after the NIE from October 2002 and weapons of mass destruction in Iraq, was to learn from that, profit and make change. And our posture, with respect -- particularly with respect to very important document, the apex of our product line of national intelligence estimates, there's no -- it's a difference of night and day.

BLUMENTHAL: I -- I appreciate the extraordinary humility of that statement, especially in light of the excellence and expertise that your organization and you personally have brought to this very, very difficult endeavor to provide and I'm quoting you, I think, "Unvarnished, untainted, timely, accurate information to the most critical national security decision that this nation makes."

And I want to express my appreciation for it and say that I think some of the disparagement has been a terrible disservice to our nation. And to the very brave and courageous men and women, who put their lives at risk so that this nation can be better informed in using our military and other force.

So I hope that we will see a change. And -- and also, join the chairman in saying that we need better policies on what constitutes a cyber attack on this nation and provide a more robust response, for example, against the Russians, not necessarily in cyber, but to impose stronger sanctions on their oil exports, on their use of foreign exchange.

The response to cyber attacks need not be one in the cyber domain. And in fact, might be even more effective if it hits their economy and their pocketbook and their livelihoods.

So Mr. Undersecretary, I appreciate your comments in that regard, I don't know whether you wanna comment in response to what I've said. And I'm out of time, so maybe we can get that in writing.

LETTRE: Mr. Blumenthal, I do wanna thank you on behalf of all the women and men of the intelligence community, I wanna thank you for that.

BLUMENTHAL: Thank you.

MCCAIN: (OFF-MIKE)

COTTON: Thank you all for appearing before us and Mr. Secretary, Director Clapper, since this is your final appearance, I know you hope.

Thank you very much for your many years of service, Director Clapper, particularly you. I'll add my voice to Senators Blumenthal and McCaskill of my administration for the men and women in our intelligence agencies.

I've had a chance as a member of the intelligence committee to meet them here at hearings and at their headquarters and around the world. And they don't get the credit they often deserve.

The troops that we help provide for in this committee usually do because they wear uniforms and they're known in public, but intelligence officers don't wear uniforms and

they're frequently undercover. So I wanna express my admiration and deepest respect and gratitude for what they do.

We've heard a lot of imprecise language here today and it's been in the media, as well, phrases like, hacked the election, undermine democracy, intervened in election. So I wanna be more precise, here.

Director Clapper, let's go to the October 7th statement. That says, quote, "The recent compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations was directed by the Russian government."

Are we talking there, specifically, about the hack of the DNC and the hack of John Podesta's e-mails?

CLAPPER: Yes.

COTTON: Are we talking about anything else?

CLAPPER: Well, that was essentially at the time, what we were talking about.

COTTON: At the time, then, we -- it says that the recent disclosures through websites like DC Leaks and WikiLeaks, are consistent with the methods and motivations of Russian-directed efforts.

DNC e-mails were leaked first, I believe in July. Is that what the statement is talking about there?

CLAPPER: I believe so.

COTTON: Mr. Podesta's e-mails, I believe, were not leaked until that very day on October 7th, so was the statement referring to that yet or was that not intended to be included?

CLAPPER: I'd have to research the exact chronology of when John Podesta's e-mails were compromised. But I think thought, that -- that bears on my statement that our assessment now is even more resolute than it was with that statement on the 7th of October.

COTTON: Thank you.

Admiral Rogers, in November at the Wall Street Journal forum, you stated quote, "This was a conscious effort by a nation-state to attempt to achieve a specific effect," end quote.

By that, did you also refer to the hack of the DNC, the hack of John Podesta's e-mail and the leaks of those e-mails?

ROGERS: Yes.

COTTON: Did you refer to anything else besides those two things?

ROGERS: Well, to be honest I don't remember the specifics of that one, particular 30-minute engagement. But clearly, as I said, what I -- what you outlined was part of my thought process.

COTTON: OK.

And then, further on in that statement Director Clapper, the intelligence community says quote, "It would be extremely difficult for someone including a nation-state actor to alter actual ballot counts or election results by cyber attack or intrusion," end quote.

And you stated that earlier today, as well that we have no evidence that no tallies were altered or manipulated in any way.

CLAPPER: That's correct.

COTTON: OK. So, that's what happened. Let's discuss why.

Director Clapper, in response to Senator Nelson, you stated that your report soon to be released will discuss the motive. Would you care to give any kind of preview today?

CLAPPER: I'd rather not.

COTTON: I didn't think so.

CLAPPER: There are actually more than one motive, so that -- that'll be described in the report.

COTTON: In your 53 years of intelligence, is ascertaining the motives, plans and intentions of foreign leaders among the hardest tasks that we ask our intelligence services to perform?

CLAPPER: It always has been.

COTTON: There's a widespread assumption -- this has been expressed by Secretary Clinton herself since the election -- that Vladimir Putin favored Donald Trump in this election.

Donald Trump has proposed to increase our defense budget, to accelerate nuclear modernization, to accelerate ballistic missile defenses, and to expand and accelerate oil and gas production which would obviously harm Russia's economy. Hillary Clinton opposed or at least was not as enthusiastic about all those measures.

Would each of those put the United States in a stronger strategic position against Russia?

CLAPPER: Certainly anything we do to enhance our military capabilities, absolutely.

COTTON: There is some contrary evidence, despite what the media speculates, that perhaps Donald Trump is not the best candidate for Russia.

OK, so that's what happened. That's why it happened, or at least a preview that we're going to know why it's happened. Let's move on to the impact.

Director Clapper, you said to Senator McCain earlier, quote, "the intelligence community cannot gauge the impact," end quote, on the election.

Is that because that kind of electoral analysis is not a task that's within the traditional responsibility and skill sets of intelligence services?

CLAPPER: That's correct.

COTTON: That's something that's more suited for someone like Sean Trende or Michael Barone or Nate Silver, election analysts that have written extensively on the election?

CLAPPER: Well, it certainly isn't the purview of the U.S. intelligence community.

COTTON: OK, thank you.

MCCAIN: (OFF-MIKE)

HEINRICH: Thank you, Chairman.

Since this will likely be the last hearing that some of you will intend -- attend in front of this committee, I just want to thank you all for your service and thank all the men and women who work for you.

I want to say a special note of gratitude to Director Clapper for 50 years of incredible service to this country.

I think what makes America great has been our ability to elect leaders through a fair, through a peaceful, and a transparent process without fear of rigging or interference in elections. And unfortunately, in this past election, we know that interference occurred.

And when I say "interference," I want to be specific. It's not about someone physically stuffing ballot boxes or someone hacking our electronic voting machines to give one candidate more votes than the other. It's about selectively and deliberately releasing damaging information in hopes of furthering one's strategic objectives; in this case, Russia's strategic objectives.

I believe this is going to happen again unless there is a price to be paid.

This interference impacts the foundation of our democracy, our elections. Which is why I welcome the sanctions against Russia announced by the president and why I believe we need to be evaluating additional Russian sanctions. It's simply too important for both parties and for the future of our country.

Secretary Lettre, given the need for deterrence in this atmosphere, which, as you said, is not always achieved by a cyber response, how important are tools like sanctions to imposing the kind of clear costs that you articulated?

LETTRE: Sanctions are a very useful tool in that toolkit.

And I think in the case of the current situation that we find ourselves in, it would be prudent to continue to look at other options to impose more sanctions on -- on Russian actors as the facts continue to develop.

HEINRICH: I would agree with that estimate and I hope that folks on both sides of the aisle will be looking at those additional tools.

For any of you who want to answer this, I'd like to know how -- how is the president-elect's at least inferred dismissive attitude towards the intelligence community broadly impacted morale in your agencies?

CLAPPER: Well, I haven't done a climate survey, but I -- I hardly think it helps it.

HEINRICH: Does anyone want to add to that?

ROGERS: I don't want to lose good, motivated people who want to help serve this nation because they feel they're not generating value to help that nation.

And I'm the first to acknowledge there's room for a wide range of opinions of the results we generate. We don't question that for one minute. And every intelligence professional knows that.

HEINRICH: Yes.

ROGERS: I've had plenty of times in my career when I have presented my intelligence analysis to commanders and policymakers and they've just looked at me and said, "Hey, Mike, thanks, but that's not the way I see it," or "You're gonna have to sell me on this."

That doesn't bother any of us. What we do I think is relevant and we realize that what we do is in no small part driven in part by the confidence of our leaders in what we do.

And without that confidence, I just don't want a situation where our workforce decides to walk, because I think that really is not a good place for us to be.

HEINRICH: I think many of us could not agree more. And if -- if the underlying facts that the intelligence community brings us are incorrect, we should call that out. I just have not seen any evidence indicating that in this case.

Oftentimes we come to different strategic or policy points of view based on that information but that's an entirely different thing.

Director Clapper, I want to go to a little bit more of not just the classified information but the relevance of publicly available information, of the whole picture of Russia's activities within the context of this election.

Can you talk a little bit about the activities of the Russian government's English-language propaganda outlets, RT, Sputnik, as well as the fake news activity we saw, as well as the social media, and how those paint a complete picture that is supplemental to what we saw with the hacking in this case?

CLAPPER: I appreciate your asking -- raising that because, while there has been a lot of focus on the hacking, this was actually part of a multifaceted campaign that the Russians mounted.

And, of course, RT, which is heavily supported by -- funded by the Russian -- the Russian government, was very, very active in promoting a particular line -- point of view, disparaging our system, our alleged hypocrisy about human rights, et cetera, et cetera. Whatever crack they could -- fissure they could find in our -- in our tapestry, if you will, they would exploit it.

And so, all of these other modes, whether it was RT, use of social media, fake news, they exercised all of those capabilities in addition to the hacking.

And, of course, I think the -- the totality of that, I think, regardless of what the impact was, which we can't gauge, just the totality of that effort, not only as DNI but as a citizen, I think is a grave concern.

HEINRICH: Thank you, Mr. Chair.

MCCAIN: (OFF-MIKE)

ERNST: Thank you, Mr. Chair.

Gentlemen, thank you very much. And I also want to thank you and the men and women that work diligently in the intelligence community (ph) for the work that they do for the United States of America.

Admiral Rogers, you've stated twice now -- you've really stressed this point -- that you must be faster and more agile in your responses.

And so, our discussion this morning will go back to a discussion that we had in September of this last year in front of this body, because I believe it is important that you understand the capabilities that exist out there and are readily available to the United States Cyber Command.

And this past September, I asked you about a Government Accountability Office report that stated "the Department of Defense does not have visibility of all National Guard unit cyber capabilities, because the department has not maintained a database that identifies the National Guard unit's cyber-related emergency response capabilities, as required by law."

And I was a bit alarmed when you stated that you haven't seen the report. It was a report that took about a year to compile and was presented to both this -- this committee and the House Armed Services Committee.

And four months later, I still have not received an answer from you, my questions, for the record. And as of this morning, all of the GAO recommendations are still open from this report.

So, it's been four months and I would just like an update on that, if you have been able to read the report and where is the department at in regards to tracking National Guard cyber capabilities.

ROGERS: Yes, ma'am.

So, first we didn't get your question until December, but I -- I acknowledge that you have formally asked us this.

First, as U.S. Cyber Command, I'm operational commander. Manning, training, and equipping is a function of services in the department.

For me in my role, I track the operational readiness levels of all National Guard and Reserve units that are allocated to the mission force. So I bore into them in the exact same way I do the active side.

In terms of more broadly, how is the department tracking this set of skills that are available, both in the reserve component? I'd argue that it's the same challenges that are in the active component. How do you take advantage of the breadth of capability that's broader than just the particular military occupational specialty, for example.

I'm the first to acknowledge that after talking to my teammates at OSD and the services, I don't think we have a good answer for you. I'll give you -- I'll something in writing for you within the next week or so because I do acknowledge that we need to do that.

ERNST: I do appreciate that because there -- how long has the United States been experiencing a tax from entities outside of the United States?

ROGERS: You could argue we've been in this cyber dynamic for over a -- a decade. I mean, it's gotten worse but...

ERNST: A decade, and so we have taken the steps of developing Cyber Command and the capabilities that exist both in our Reserves, National Guard and the active component units. And to become more faster -- or faster and more agile, we need to know what those capabilities are.

So if you have a solution to that on how we can track those capabilities, we need to figure that out. Many of these units have the capability of defending networks and yet we're not utilizing those capabilities. And we don't know where they exist, to be honest.

ROGERS: So please don't take from my comment that we don't believe that the role of the Guard and Reserve isn't important. If you look at in the last 12 months, we've got two cyber protection teams from the Guard that have been mobilized. We're -- we've gone online in the Guard and the Reserve national mission teams for the first time within the last year. I mean it's great to see how Guard and Reserve are developing more and more capability. That's a real strength for us...

(CROSSTALK)

ERNST: Absolutely, and I think we'll see those continue develop even more in the future, but we need to be able to utilize those capabilities that exist out there. So, you know, that many of our best soldiers in the National Guard and Reserves come from the

private sector. I know this from some of my own Guardsmen that worked full time in computer technology and cyber technology.

And you were -- you stated in September you were trying to figure out how better leverage the National Guard and do you have a response for that? Have you thought of ways that we might be able to use those Guard units more readily?

ROGERS: This is a topic that in fact I was just talking to General Lengyel the -- the director of the Guard Bureau a few weeks ago to say, hey look, this is something in 2017 I want us to sit down -- I think there's a couple specific missionaries where the capabilities of the Guard and Reserve are really well optimized. Because I'd be the first to admit, the answer can't be every time, we'll just throw the active component at this. I don't think that's an optimal approach for us to do in business.

So you'll see this play out for us in 2017, we gotta work through Title 32 versus Title 10 issue. What role -- what's the right way to do this?

ERNST: Absolutely.

ROGERS: Do we put it within the defense support to civil authority construct? I'd like that because it's a framework that we already have. I'm a big fan of let's not reinvent the wheel when it comes to cyber. How do we take advantage of process into structures and authorities that are already in place? That's one thing you'll see some specific changes on within a department we're working through right now on the policy side.

ERNST: Very good. Well, I appreciate it. I know my time is expiring. So, I look forward to working with you on that, Admiral Rogers.

MCCAIN: (OFF-MIKE)

DONNELLY: Thank you, Mr. Chairman.

And I want to thank all of you for all your efforts today, for the amazing careers you've had.

And, Mr. Chairman, thank you for holding this hearing, I think it's critically important to our nation.

And I want to be clear that the purpose of today's hearing is not to debate the validity election, but to discuss foreign attempts to use cyber attacks, to attack our country, including the recent Russian actions intended to influence our elections.

And I appreciate the bipartisan effort to get our people the answers they deserve. And I'm grateful for the amazing efforts that our intelligence agencies put forth, every single day. That every day, lives are on the line to make sure that we're safe and to make sure that all Americans have a chance to take care of their families and go to sleep at night and not have to worry while your people are on the front lines all around the world.

DONNELLY: And I can tell you on behalf of all Hoosiers that when it comes down to a choice between your people or intelligence agencies, and Julian Assange, we're on your team every time. And I actually find it stunning that there's even a discussion in our country about the credibility of our intelligence agencies versus Mr. Assange.

It -- it is astounding to me that we would even make that comparison, when you see the stars in the CIA headquarters of all the people who have lost their lives and who have lost their lives in their agencies to keep us safe.

Director Clapper, how would you describe your confidence in attributing these attacks to the Russian government opposed to someone in their basement?

CLAPPER: It's very high.

DONNELLY: The government has named those responsible for the DNC hacks as APT 28 and APT 29, part of the Russian intelligence services, the GRU and the FSB. Are all the actors targeted by these two entities known to the public sir?

CLAPPER: I'm sorry sir, the question again? Are all what?

DONNELLY: All the actors in the -- targeted by these two entities GRU, the FSB, APT 28, APT 29. Do we know everybody? Have you told us who is involved or are there more that you can't discuss at this time?

CLAPPER: Right, I don't think I can discuss that in this forum.

DONNELLY: OK. How -- how far up the chain is -- in what you can tell us, does this go in regards to the Russians? At what level were the instructions to take these actions given?

CLAPPER: Again sir, I can't speak to that in this setting.

DONNELLY: Thank you.

Do you think we are communicating clearly to our adversaries in a language that they'll understand? That the costs will outweigh any gains that they get if they try this again? Not only you Director, but the others, how do we best send that message do you think?

CLAPPER: Well, certainly the sanctions that were -- that have been imposed, the expulsion of the intelligence -- the 35 intelligence operatives, the closure of the two facilities which were used for intelligence purposes and the other sanctions that were levied, I think does convey a message. There's -- it's open to debate whether more should be done. I'm a big fan of sanctions against the Russians, but that's just me.

DONNELLY: Admiral, what would you say sir?

ROGERS: I would agree. I mean the challenge here is look, we don't want -- I don't think it's in the best interest of any of our nations to be in the confrontational approach to doing business. And, we've got to figure out how do we articulate what is acceptable, what is not acceptable in a way that enables us to continue to move forward in a productive relationship.

That's not unique to the Russians, I would argue that that's a challenge for us on a whole host of actors out there. This is just in some ways been the poster child for this challenge of late.

CLAPPER: I would add to that if I may that -- it certainly would be a good thing if we could find areas where our interests converge. I'm speaking of ours and the Russians, and we've done that in the past. So, to -- just to (inaudible) Admiral Rogers' point. But there's -- I there is a threshold of behavior that's just unacceptable. And, somehow that has to be conveyed.

DONNELLY: Well, I am out of time, but on behalf of all the American people we want to thank you. You have dedicated your lives to keeping us safe and we're incredibly grateful for it.

Thank you Mr. Chairman.

MCCAIN: (OFF-MIKE)

SULLIVAN: Thank you, Mr. Chairman and thank you, for you and the ranking member for holding this hearing.

And, I also want to thank you, General Clapper, Mr. Secretary for your service as this might be your last hearing, and the men and women you lead.

You know, you describe in your testimony the increasing attacks we're seeing, not just from Russia, but China and other actors, Iran, North Korea, their increasing capabilities. The chairman's opening statement pretty much stated that it's his view, and I certainly share the view that we're being hit repeatedly because the benefits outweigh the costs for those who are taking these actions against us. Do you agree with that?

CLAPPER: I do. And I think -- I think we all do that this is for adversaries like -- I'll just name, North Korea and Iran, it is a very relatively low cost acts that can cause havoc. And what I think we've seen over time is that they -- they keep pushing the envelope as they -- as their capabilities improve and they're willing to exercise those capabilities.

SULLIVAN: So if that's the case, and I -- it's glad that I think there's some consensus here. You're talking about retaliating, upping the cost with all instruments of power. Mr. Secretary you mention retaliate at a time of our choosing -- in the realm of our choosing, but it doesn't seem to be happening -- it doesn't seem to be happening because the attacks continue.

So let me just give an example. Let's say Iran conducted -- and you mentioned that they're being more aggressive, more risky than North Korea -- some kind of cyber attack. If we did something, maybe without announcing it, like the president announced the Russian counter actions.

But let's say we didn't announce it. Let's say we did something where we essentially collapse their financial system. Or something pretty dramatic and we let them know we did it, but we don't have to publicize it.

Do you think that's the kind of action that would say, hey don't do this or we're going to come back and retaliate at our time, our choosing and crush you. How come we haven't done that yet? And do you think that if we did something like that with the Iranians or the North Koreans would that -- would that deter them in the future?

Mr. Secretary?

LETTRE: Senator I think you're getting right at the question of what is the -- what do we mean by a proportional response in some instances.

SULLIVAN: Or asymmetric right? You're talking about asymmetric responses which I fully agree with.

LETTRE: That's right or in instances that are significantly serious and grave, whether a more than proportional response is required to really set that deterrence framework in place.

SULLIVAN: But isn't the key question right now and it came from the Chairman's opening statement, which I think you agreed with, is that nobody seems to be intimidated by us right now. So let me give another example.

Senator Inhofe asked a question early on about China. China hacked, allegedly -- maybe you can confirm that -- government lead, 22 million files. A lot of the SF 86 files that you used for background clearances, they hacked -- they have mine I was informed by the government. Very sensitive information as you know that they can use against intelligence operatives and military members.

And Senator Inhofe asked the question, did we retaliate -- what did we do? The answer that I heard from all of you was, well we try to protect people, like me, and I'm sure others who's sensitive intel information and background information was compromised.

But I didn't hear any claim of a retaliation on a huge hack. Huge, 22 million American, federal, military, intel workers got hacked by the Chinese.

So the president signed this statement with President Xi Jinping, the U.S.-China Security Agreement. But obviously Mr -- or General Clapper, from your testimony the Chinese have not abided by that, have they?

CLAPPER: They have, as I indicated in my testimony..

(CROSSTALK)

SULLIVAN: I thought you said they were continuing to deal.

CLAPPER: I'm sorry?

SULLIVAN: I'm sorry, I thought you said in your testimony today that they continue to conduct cyber attacks.

CLAPPER: They continue to conduct cyber-espionage. They have curtailed, as best we can tell. There has been a reduction and I think the private sector would agree with this. There has been some reduction in their cyber activity.

And the agreement simply called for stopping such exfiltration for commercial gain.

SULLIVAN: So let me just ask a final question. Did we retaliate? And up the cost against China after an enormous cyber attack against our nation?

CLAPPER: We did not retaliate against an act of espionage anymore than other countries necessarily retaliate against us for when we conduct espionage.

SULLIVAN: But isn't that answer just part of the problem, that we're showing that we're not going to make it costly for them to come in and steal the files of 22 million Americans, including many intel officers?

CLAPPER: Well, it's as I say, people who live in glass houses need to think about throwing rocks. Because this was -- this was an act of espionage and, you know, we and other nations conduct similar acts of espionage. So if we're going to punish each other for acts of espionage, that's a -- that's a different policy issue.

MCCAIN: Senator King?

KING: Thank you, Mr. Chairman. Your opening statements are always erudite and thoughtful, but I thought today's was particularly so. Very -- you touched on all the important points that have really formed the basis for this hearing so I -- I want to thank you for that.

Director Clapper, I think it's important to put some context around some of these discussions. One of the most important things to me is that your public statement in October, along with Jeh Johnson was prior to the election and you were simply telling facts that you had observed and, in my experience of reading intelligence community communications, it's one of the more unequivocal that I've seen.

You've stated here you have high confidence in those conclusions that the Russians were behind it. That it was intended -- intended to interfere with our elections and that approval went to the highest levels of the -- of the Russian government. Have you learned anything subsequently that you can tell us here today to contradict those findings that you publicly stated last October?

CLAPPER: No. In fact, if anything, what we've since learned just reinforces that statement of -- of -- of the 7th of October.

KING: And there was no political intention? You were simply reporting facts as you saw them. I presume that's correct? Your -- your history is one of being non-political.

CLAPPER: Absolutely. I felt particularly strongly, as did Secretary Johnson, that we owed it to the American electorate to let them know what we knew.

KING: Now, people in Maine are skeptical and they want to have evidence and proof and I'm hearing from people, prove it. The problem, as I understand it, is the desire to provide evidence that is convincing that your conclusions are correct versus the danger of compromising national security on sources and methods. Can you, sort of, articulate that, because I think that's an important point.

CLAPPER: We have invested billions and we put people's lives at risk to glean such information. And so if we were to fulsomely expose it in such a way that would be completely persuasive to everyone, then we can just kiss that off because we'll lose it.

And then that will endanger our -- imperil our ability to provide such intelligence in the future. And that's all that -- the dilemma that we have in intelligence. We want to be as forthcoming and transparent as possible, but we feel very, very strongly, as we do in this case, about protecting very fragile and sensitive sources and methods.

KING: Let's again turn to a question of context.

What we saw in this country this fall and in the -- going back actually almost a year, was -- was -- was a example of a Russian strategy that's been playing out in Europe for some time that includes, not just hacking, as you said, but disinformation, propaganda -- I heard just from a senior commander -- I took a break here from the hearing -- in Europe, that Russia is actually buying commercial TV stations in Western Europe at this point.

And this is a comprehensive strategy that we've seen playing out in Eastern Europe and also there was a report this morning that they are funding one of the candidates for the presidency of France in the election this May.

CLAPPER: Well, the Russians have a long history of interfering in elections. Theirs and other people's. And the difference -- and there's a long history in this country of disinformation. This goes back to the 60's, the heyday of the Cold War. Funding that they would share or provide to candidates they supported, the use of disinformation, but I don't think that we've ever encountered a more aggressive or direct campaign to interfere with our election process than we've seen in this case.

KING: And channel -- there are so many more channels of disinformation today than there were in the past.

One final point...

CLAPPER: That's exactly right and that's a very key point about the -- of course the cyber dimension and social media and all these other modes of communication that didn't exist in the -- in the Cold War.

KING: One final point. We -- we had a meeting with the committee with a group of representatives from the Baltic States, and I know the Chairman was just in the Baltic States. I asked them -- and they are just deluged with this.

I mean they warn -- have warn -- been warning us about this for years about the messing around with elections. I -- I said, so what do you do? How do you defend yourself?

And they said, well, we're trying to defend ourselves in various ways. But the best defense is for our public to know what's going on so they can take it with a grain of salt. I thought that was a very interesting observation because their people now say, oh yeah, that's just the Russians.

That's why I think public hearings like this -- and -- and the -- the public discussion of this issue is so important because we're not gonna be able to prevent this all together. But we need to have our people understand that when they're being manipulated. Would you agree with that conclusion?

CLAPPER: Absolutely. That's why I feel so strongly about the statement in October.

KING: Thank you.

Thank you, Mr. Chairman.

MCCAIN: Just to follow up, Chairman Clapper, during the Cold War we had a strategy and we had Radio Free Europe, and we had the Voice of America -- Senator Graham, who will be speaking next, will attest that when our recent trip, they don't have a strategy. They don't have a counter propaganda -- the United States of America I'm talking about.

And we've got to develop that strategy, even if it encompasses the internet and social media. But they -- they are -- they are doing pretty significant stuff, particularly in the Baltics and Eastern Europe. Would you agree, Senate Graham?

GRAHAM: Yes. Appreciate being before the Committee. Thank you.

So, yes, I would. Would you agree with me that Radio Free Europe is outdated?

CLAPPER: I -- frankly not up on...

GRAHAM: Well, it says radio...

(CROSSTALK)

GRAHAM: ... and a lot of people don't listen to the radio like they used to. OK.

CLAPPER: Well, actually radio's is a -- is a -- a very popular mode in many parts of the world.

GRAHAM: Radio's big in your world?

CLAPPER: In my world?

GRAHAM: Yeah.

CLAPPER: Not so much.

GRAHAM: Yeah, I don't listen to the radio much either. So, the bottom line is you're gonna be challenged tomorrow by the president- elect. Are you OK with being challenged?

CLAPPER: Absolutely.

GRAHAM: Do you both welcome it?

CLAPPER: We do.

GRAHAM: Do you think it's appropriate?

CLAPPER: We do.

GRAHAM: Are you ready for the task?

CLAPPER: I think so.

GRAHAM: Good. Is there a difference between espionage and interfering in an election?

CLAPPER: Yes. Espionage implies a -- to me at least, a passive...

GRAHAM: Yeah, OK.

CLAPPER: ... passive collection, and this was much more activist.

GRAHAM: So, when it comes to espionage, we'd better be careful about throwing rocks. When it comes to interfering in our election, we better be ready to throw rocks. Do you agree with that?

CLAPPER: That's a good metaphor.

GRAHAM: I think what Obama did was throw a pebble. I'm ready to throw a rock. Would I be justified as a United States Senator, taking your information about Russia's involvement in our election and what they're doing throughout the world and be more aggressive than President Obama if I chose to?

CLAPPER: That's your choice, Senator.

GRAHAM: Do you think he was -- he was justified in imposing new sanctions based on what Russia did?

CLAPPER: I do.

GRAHAM: OK. So, to those of you who want to throw rocks, you're gonna get a chance here soon. And if we don't throw rocks, we're gonna make a huge mistake.

Admiral Rogers, is this gonna stop until we make the cost higher?

ROGERS: We have got to change the dynamic here because we're on the wrong end of the cost equation.

GRAHAM: Yeah, you got that right. Could it be Republicans next elections?

ROGERS: Could -- this is not about parties per se.

GRAHAM: Yeah, it's not like we're so...

(CROSSTALK)

GRAHAM: ... much better at cybersecurity than Democrats, right.

Now, I don't know what Putin was up to, but I don't remember anything about Trump in the election. Now, if Trump goes after the Iranians, which I hope he will, are they capable of doing this?

ROGERS: They clearly have a range of cyber capability. And they have been willing to go offensively both -- we've seen that in the United States in the...

(CROSSTALK)

GRAHAM: So, if Trump takes on China, which I hope he will, are they capable of doing this?

ROGERS: Yes.

GRAHAM: OK. So, we got a chance as a nation to lay down a marker for all would-be adversaries. Do you agree with that?

ROGERS: Yes. And I'd be the first to acknowledge we think -- need to think about this broadly.

GRAHAM: Yeah. And we should take that opportunity before it's too late.

ROGERS: Yes, sir.

GRAHAM: Do you agree -- agree with me that the foundation of democracy is political parties. And when one political party is compromised, all of us are compromised.

ROGERS: Yes, sir.

GRAHAM: All right. Now, as to what to do. You say you think this was approved at the highest level of government in Russia, generally speaking, is that right?

CLAPPER: That's what we said.

GRAHAM: OK. Who's the highest level of government?

CLAPPER: Well, the highest is -- is President Putin.

GRAHAM: Do you think a lot happens in Russia, big, that he doesn't know about?

CLAPPER: Not very many.

GRAHAM: Yeah, I don't think so either.

CLAPPER: Certainly none that are politically sensitive in another country.

GRAHAM: OK. Now as we go forward and try to deter this behavior, we're going to need your support, now and in the future. So I want to let the president-elect know that it's OK, to challenge the intel. You are absolutely right to want to do so.

But what I don't want you to do is undermine those who are serving our nation in this arena until you are absolutely sure that they need to be undermined. And, I think they need to be uplifted not undermined.

North Korea, let me give the example of real world stuff that he's going to have to deal with, Trump. Do you believe that North Korea is trying to develop an ICBM to hit the United States or that could be used to hit the United States?

CLAPPER: That could be, yes.

GRAHAM: Do you agree with that Admiral Rogers?

ROGERS: Yes.

GRAHAM: So when the -- or the North Korean leader says that they are close to getting ICBM, he's probably in the realm of truth?

ROGERS: He's certainly working aggressively to do that.

GRAHAM: And, if the president of the United States says it won't happen, he's going to have to come to y'all to figure out how far along they are because you would be his source for how along they are. Is that right?

ROGERS: I'd hope we'd be part of that process.

CLAPPER: I'd hope we'd be the source.

GRAHAM: Yeah, I hope he would talk to you too. And, here's what I hope he realizes. That if he has to take action against North Korea, which he may have to do. I intend to

support him. But he needs to explain to the American people why. And one of the explanations he'll give is based on what I was told by the people who are in the fight. And, let me tell you this, you don't wear uniforms, but you're in the fight. And, we're in a fight for our lives. I just got back from the Baltics, Ukraine and Georgia, if you think it's bad here, you ought to go there.

So ladies and gentlemen, it is time now not to throw pebbles, but to throw rocks. I wish we were not here. If it were up to me we would all live in peace, but Putin is up to no good and he better be stopped. And, Mr. President-elect, when you listen to these people you can be skeptical but understand they are the best among us and they are trying to protect us.

Thank you all.

MCCAIN: Do you have any response to that diatribe?

(LAUGHTER)

CLAPPER: (OFF-MIKE)

(UNKNOWN): Microphone.

CLAPPER: Senator Graham have had our innings before, but I find myself in complete agreement with what he just said and I appreciate it.

GRAHAM: Thank you.

CLAPPER: Senator -- Chairman McCain, if I might, just pick up on a comment of yours. And, that has to do with the information fight if you will. And, this is strictly personal opinion, not company policy, but I do think that we could do with having a USIA on steroids. United States Information Agency to fight this information war that -- a lot more aggressively than I think we're doing right now.

MCCAIN: You know I agree General and I think one of the areas it's -- where we're lacking and lagging more than any other area is social media. We know these young people in the Baltics are the same as young people here, they get their information off the internet and we have really lagged behind there.

Senator Gillibrand?

GILLIBRAND: Thank you, Mr. Chairman, and Mr. Ranking Member for hosting this very important hearing.

I want to follow on some of the questioning that Senator Ernst started concerning the National Guard and cyber. I have been pushing DOD to use the Guard for years, and appreciate that this is beginning to happen. Members of the Guard bring unique skills and capabilities and we should be leveraging them.

Admiral Rogers, I look forward to working with you on how best to do this. Can you tell me whether there has been movement on the Army National Guard Cyber Protection Teams being included in the cyber mission forces?

ROGERS: Yes. And, we've brought two online that have been activated in the last year. Two additional that are coming online in '17, the first of which just came online. So yes ma'am.

GILLIBRAND: And, how much more is left to be done and when do you expect it to be done?

ROGERS: The Guard and the Reserve are bringing on an additional 21 teams. Those will not be directly affiliated with the mission force. But one of the things -- one of the things I think we're going to find over time, the only way to generate more capacity in a resource constrained world, is to view this as an entire pie, not just, "Well, here's one sliced-off area that -- the mission force and here's a separate area (OFF-MIKE)."

I think what we're gonna be driven to is we're gonna have to look at this as an integrated (ph) whole.

GILLIBRAND: I do too. Because at the end of the day, our Guard and Reserve, they have day jobs and they may be working at Google and Microsoft and Facebook and all these technology companies that have extraordinary skills. And as a way to tap into the best of the best, I think we should look at people who already have these skills, who are already committed to serving our nation as best we can.

ROGERS: Right.

GILLIBRAND: So I appreciate your work.

ROGERS: Yes, ma'am.

And if I could, one area that I'd be interested in your help in, for many employers in the Guard and the Reserve, and I say this as the son of a Guardsman, when I was a kid growing up, they often, sometimes, tend to view that service as something that you do overseas. "Hey, I'm willing to let you go because you're going to Afghanistan and going to Iraq."

And in the world of cyber, we are operating globally from a -- you know, from a garrison, pick the location...

(CROSSTALK)

GILLIBRAND: From any location in the world.

ROGERS: ... anywhere, and...

GILLIBRAND: Correct.

ROGERS: So this -- I'm -- I was, this just came up -- General Lengyel and I were just talking about this yesterday, as a matter of fact, where I said one of the things we need to do is educate employers about what is the nature of this dynamic, and it's every bit as relevant as, "Hey, we're sending somebody to Afghanistan or Iraq."

GILLIBRAND: I think that's right.

On a separate topic, but related, I've been long advocating for aggressive development of the manpower that we need to support our cybersecurity mission. In particular, I continue to believe that we have to not only develop the capability in our military and the interest in cyber among young Americans, but that the military must be creative when thinking about recruitment and retention of cyber warriors.

How would you assess our current recruitment and retention of cyber warriors? And what challenges do you foresee in the future, and what recommendations do you have to address them?

Because, obviously, we are competing with some of the most dynamic, innovative companies in the world. But we need them to be our cyber defense and our cyber warriors.

ROGERS: So knock on wood, in the military aspect, we are exceeding both our recruiting and retention expectations. I worry about how long can we sustain that over time under the current model.

My immediate concern is a little less on the uniform side, in part because money -- if money was a primary driver for them, they wouldn't have come to us in the first place.

On the civilian side, however, that's probably my more immediate concern. I'm finding it more challenging -- we're able to recruit well, retaining them over time. I'm really running into this on the NSA side, right now. But how do you retain high-end, very exquisite civilian talent for extended periods of time?

GILLIBRAND: Well, I'd be delighted to work with you over the next year on that.

ROGERS: Yeah.

GILLIBRAND: Director Clapper, I was very interested in your opening remarks and the initial conversation you were having about the Russian hack onto the DNC and to various personnel's e-mails and the question of whether it was a declaration of war.

And -- and given that that is such a serious statement, I wanna ask you, do you think we should take things like the Democrat/Republican Party infrastructure and consider them to be critical infrastructure? Should we actually be looking at our infrastructure differently since -- because of this recent event?

CLAPPER: That's been the subject of discussion about whether, you know, our political infrastructure should be considered critical infrastructure. I know Secretary Johnson's had discussion with state officials about that. There is -- there is some pushback on doing that.

So it's a policy call. Whatever additional protections that such declaration would afford, I think that would be a good thing. But whether or not we should do that or not is really not a call for the intelligence community to make.

GILLIBRAND: Well, I hope it's one that the members here in this committee will discuss, because, if it is -- if it does result in such a grave intrusion, maybe it should be critical infrastructure. And certainly, politics and political parties are not set up that way. And so it would be quite a significant change.

Thank you.

MCCAIN: Director Clapper has to leave in about 20 minutes, so we will enforce the crime -- the time...

(LAUGHTER)

... the time.

Senator Tillis?

TILLIS: Thank you, Mr. Chair.

And, gentlemen, thank you all for your service. I, for one, have high confidence in the community that you represent, and I hope that they recognize that I speak for most of the senators here that share the same view.

TILLIS: Director Clapper, I'm gonna spend most my time probably reflecting on some of the comments that you've made. The glass house comment is something I think's very important.

There's been research done by a professor up at Carnegie Mulligan -- Mellon that's estimated that the United States has been involved in one way or another in 81 different elections since World War II. That doesn't include coups or regime changes, so tangible evidence where we've tried to effect an outcome to our purpose.

Russia's done it some 36 times. In fact, when Russia apparently was trying to influence our election, we had the Israelis accusing us of trying to influence their election.

So, I'm not here to talk about that, but I am here to say that we live in a big glass house and there are a lot of rocks to throw. And I think that that -- that's consistent with what you said on other matters.

I want to get back to the purpose of the meeting, the foreign cyber threats. I think Admiral Rogers and Director Clapper, you all have this very difficult thing to communicate to policy people who may not have subject matter expertise in this space.

For example, Director Clapper, you were saying that one of the problems with a counterattack -- I think it was you; it could have been Admiral Rogers -- is that you may have to use an asset that's actually a presence on some other nation where that nation may or may not know that we have a presence there.

In fact, we have presences across cyberspace that are not known, that as a part of the counterattack -- that part of the counterattack could be nothing more than exposing our presences, because we know a lot of our adversaries may or may not be aware of presences that we have out there in appropriate locations. Is that correct?

CLAPPER: Yes.

And I think you've succinctly illustrated the complexities that you run into here.

TILLIS: So that is why, as thrilling as somebody who's written the precursors to phishing code before and stolen passwords as part of ethical hack testing, so I was paid to do this, that underscores the need for us to really be educated about the nature of this battlespace and how more often than not it's probably more prudent to seek a response that isn't a cyber response given the fluid nature.

I mean, we're in an environment now where we build -- we see a threat and we build a weapon system. It's on the water, it's in the air, it's on the ground. And then we kind of counter that threat and we come up with war plans to use that capability.

In cyberspace, major weapons systems get created in 24-hour cycles. You have no earthly idea whether or not you have a defensive capability against them.

So, if you all of a sudden think, "Let's go declare war in cyberspace," be careful what you ask for, because collectively, you could have -- there are 30 nations right now that have some level of cyber capability. There are four or five of them that are near-peer to the United States. There are two or three that I think are very threatening, and in some cases probably have superior capabilities to us in terms of presences. Maybe not as sophisticated but potentially, in a cyber context, more lethal.

So, I think, you know, there are a lot of questions -- one of the beauties of being a freshman -- I guess now I'm not a freshman -- being at the end of the dais, all the good questions have been asked.

(LAUGHTER)

But one of the things that I would suggest that we do, is we as members really get educated on the nature of this threat and the manner in which we go about fighting it and understanding that the -- the iterative nature of weapons creations on the internet are unlike anything we've seen in recorded human history for warfare. And we need to understand that.

We also need to understand what the rules of engagement are going to be and how future AUMFs actually include a specific treatment for behaviors that are considered acts of war and then a whole litany of things that we should do for appropriate responses so that we can begin to make more tangible the consequences of inappropriate behavior in cyberspace.

And so that's not so much a diatribe but it probably is a speech, Mr. Chair.

The last thing I'll leave you with is, Admiral Rogers, I'd like for my office to get with you and continue to talk about how we get these bright people retained and recruited to stay up to speed with developing these threats. We need to understand that they are -- they are the secret to creating these weapons systems to counter the malicious acts like Russia, China, Iran and a number of other nations that are trying to develop against us.

Thank you.

MCCAIN: Senator Hirono?

HIRONO: Thank you, Mr. Chairman.

And thank you, gentlemen, for your service.

I -- I think it's clear that we have tremendous concerns about the Russian hacking in our elections. And I think it's more than ironic that we have a president-elect who kept talking about our elections being rigged, which I would consider trying to interfere with

our elections to be a part of a rigged kind of an election. At the same time, he denied Russians' -- Russia's activities in this regard.

As some of this was already touched on, regarding the president-elect's attitude towards the intelligence community, the morale that -- the impact on morale.

So, going forward, as we are challenged by the need to have more cyber-aware or skilled cyber workforce, if this attitude toward the intelligence community doesn't change on the part of decision-makers, including the president, would you agree that it would make it that much harder, Director Clapper and Admiral Rogers, to attract the kind of cyber-experienced workforce that we need to protect our country?

CLAPPER: Well, it could.

I don't know that we could say it's -- the -- all -- some of these statements have had any impact on recruiting...

HIRONO: Or retention.

CLAPPER: It could. I think it could.

On retention, I think -- just maybe embellish what Admiral Rogers was saying, I do think that consideration needs to be given to having more flexibility, more latitude on compensation for our high-end cyber specialists who are lured away by industry, who're paying huge salaries. That's not why you're in the government, not why you serve in the intelligence community is not, obviously, for money.

But I do think that in those highly technical, high-end skill sets that we -- we badly need in the government, in the intelligence community, that it would be helpful to have more latitude on compensation as Mike was...

ROGERS: And I would agree...

HIRONO: Very briefly.

ROGERS: ... that both of these individuals (inaudible) within the last 24 hours (inaudible) using my authority as the director of NSA, I am going to authorize the

following increased compensations for the high-end cyber part of our workforce, because I am just watching the loss (ph)...

HIRONO: Yes, of course.

And it's not just compensation that attracts people to what we're doing in our intelligence community, because service to the country is a very important motivation and, of course, I would think that morale would be very much attendant to that.

There was some discussion about what would constitute in the cyber arena an act of war. And, Director Clapper, I note in your testimony that I think that this is one of the reasons that we want to develop international norms in this arena.

So, who should be the key players in developing and agreeing to these international norms in the cyber arena?

And if the big players are U.S., China, Russia, if we don't have those players at the table to come up with these international norms, how realistic is it to develop and -- and adhere?

CLAPPER: Well, that's exactly the challenge. And those are the key nation-states that would need to engage.

And there has been work done under the auspice of the United Nations to attempt to come up with cyber norms but I think we're a ways away from those having -- having impact.

HIRONO: Would you agree, Admiral Rogers?

ROGERS: Yes, ma'am.

HIRONO: Turning to the awareness of the public as to the extent of the threat, a 2016 opinion piece by two members of the 9/11 Commission, basically they said that the most important thing government and leaders in the private sector can do is to clearly explain how severe this threat is and what the stakes are for the country.

So, Director Clapper, do you think that the general public understands the severity of the cyber threat and the stakes for the country?

And what should Americans keep in mind with regard to this threat? And what can ordinary Americans do to contend with this threat?

CLAPPER: I think there's always room for more -- more education. And certainly we have a role to play in the intelligence community in sharing as much information as we can on threats posed by both nation- states as well as non-nation-states.

And I think there are simple things that Americans can do to protect themselves. You know, be aware of the threat posed by spear phishing, for example, which is a very common tactic that's used yet today. We have a challenge in the government getting our people to respond appropriately to cyber threats.

So this is one case where communicate, communicate, communicate is -- is the watch word.

MCCAIN: Senator Cruz?

CRUZ: Thank you, Mr. Chairman.

Gentlemen, thank you for being here. Thank you for your service to our nation.

The topic of this hearing, cybersecurity, cyber attacks, is a growing threat to this country and one that I think will only become greater in the years ahead. We have seen in recent years, serious attacks from among others, Russia, China, North Korea.

Indeed it is with some irony, I spent a number of years in the private sector and to the best of my knowledge never had my information hacked and then all I had to was get elected to the United States Senate and the office of personnel management was promptly hacked and everyone on this bench had our information stolen by a -- by a foreign assault.

My question, Admiral Rogers, starting with you is, what do you see as the greatest cybersecurity threats facing our country and what specifically should we be doing about it to protect ourselves?

ROGERS: So a small question.

(LAUGHTER)

When I look at the challenges and the threats, it's in no particular order. Significant extraction of information and insight that is generating economic advantage for others, that is a routine (ph) operational advantage at times for us as a nation. That is as you have seen in this Russian piece where not just the extraction, but then the use of this information as a whole other dimension.

And what concerns me beyond all that is, what happens if we start to move in an environment in which, not only is information being, I've heard some people use the phrase weaponized, what happens when now we start peoples -- we see people suddenly manipulating our network, so we can't believe that data that we're looking at.

That would be a real fundamental game changer to me and to me it's only a question of the when, not the if this is going to happen. And what happens when the non-state actor decides that cyber offers an asymmetric advantage to them because their sense of risk and their willingness to destroy the status quo is significantly different and greater than a typical nation state. Those are the kinds of long-term things.

So as we've talked about more broadly today, we've gotta get better on the defensive side. Because part of deterrence is making it harder for them to succeed, I acknowledge that. But a defensive strategy alone isn't going to work. It is a resource intensive approach to doing business and it puts us on the wrong end of the cost equation. That's a losing strategy for us, but it is a component of the strategy.

We have got to ask ourselves, how do we change this broader dynamic to go to the point you've heard repeatedly today, how do we convince nations and other actors out there that there's a price to pay for this behavior. That in fact it is not in your best interest...

CRUZ: And what should that price be?

ROGERS: Oh, it's a wide -- it's a wide range of things here. There's no one silver bullet, which is another point I would make. If we're looking for the perfect solution, there isn't one. This will be a variety of incremental solutions and efforts that are going to play out over time. There is no one single approach here.

CRUZ: Wow, and your point about manipulating data, about a month ago I chaired a different committee -- a hearing on artificial intelligence and our growing -- economies

growing reliance on artificial intelligence and one of the things that the witnesses testified there was concern on the cybersecurity side of a hack that would modify the big data that is being relied on for artificial intelligence to change the decision making in a way that no one's even aware it's been changed and I think that's a -- a threat.

I hope that -- that y'all are examining closely and it's the sort of threat that could have significant repercussions without anyone even being aware that it's happening.

Let me shift to a -- to a different topic. Director Clapper, you've testified before this committee that Cuba's an intelligence threat on -- on par with Iran and listed below only Russia and China. And there're reports that the Lourdes, the Russian operated signal intelligence base in Cuba, will be reopened and then additionally this past summer Russia and Nicaragua struck a deal to increase military and intelligence cooperation.

And resulting in an influx of Russian tanks into Managua and a agreement to build an electronic intelligence base which maybe disguises satellite navigation tracking station. To the best of your knowledge, what is Russia's strategy in the Western Hemisphere and how are concerned are you about the Russians expanding their influence in Cuba and Nicaragua?

CLAPPER: Well, the Russians are bent on establishing both a presence in -- in the Western Hemisphere and they're looking for opportunities to expand military corporation, sell equipment, air bases, as well as intelligence-gathering facilities. And so it's just another extension of their aggressiveness in pursuing these interests.

And with respect to Cuba, Cuba's always had a long-standing very capable intelligence capabilities. And I don't see a reduction of that of -- of -- of those capabilities.

CRUZ: Thank you.

MCCAIN: (OFF-MIKE)

KAINE: Thank you, Mr. Chair.

And thanks to the witnesses for today and for your service.

And, Mr. Chair, I appreciate you calling this hearing. I think hearing is a test of this body, the Article I branch, Congress, this hearing and others to follow.

I was chairman of the Democratic National Committee for a couple of years. And we had a file cabinet in the basement that had a plaque over it. It was a file cabinet that was rifled by burglars in an invasion of the Democratic National Committee in 1972. It was a bungled effort to take some files and plant some listening devices.

That small event led to one of the most searching and momentous congressional inquiries in the history of this country. It was not partisan.

One of the leaders of the congressional investigation was a great Virginian, Caldwell Butler -- who was my father-in-law's law partner in Roanoke, Virginia, before he went to Congress -- played a major role.

It was not an investigation driven because something affected the election. The 1972 presidential election was the most one-sided in the modern era.

But it was a high moment for Congress because Congress in a bipartisan way stood for the principle that you couldn't undertake efforts to influence an American presidential election and have there be no consequence.

The item that we'll discuss and we'll discuss more when the hearing comes out is -- is different. That was a -- a -- a burglary of a party headquarters that was directed to some degree from the office of the president. But this is very serious.

The combined intelligence of this country has concluded that efforts were undertaken to influence an election by and adversary, an adversary that General Joe Dunford, the head of the Joint Chiefs of Staff, said in testimony before this hearing was the -- in his view, the principal adversary of the United States at this point. In addition, the attack was not just a party headquarters.

The October 7 letter that you've referred to talked about attacks on individuals, current and former public officials of -- with significant positions, and also attacks on State Boards of elections. The letter of October 7 traced those attacks to Russian entities -- Russian companies and didn't ascribe at least in that letter that -- to directed by the Russian government. But I'm curious about what the full report will show.

It is my hope that this Congress is willing to stand in a bipartisan way for the integrity of the American electoral process and will show the same backbone and determination to

get all the facts and get them on the table as the Congress did in 1974. There was another Congressional inquiry that was directed after the attacks on 9/11.

And there was a powerful phrase in that report that I just want to read. The commission concluded quote, "The most important failure was one of imagination. We do not believe leaders understood the gravity of the threat." And that's something I think we'll all have to grapple with.

Did we have sufficient warning signs? I think we did. And having had sufficient warning signs, why did we not take it more seriously?

That question is every bit as important as a question about what a foreign government, an adversary did and how we can stop it from happening.

Three quick points. One, is the report next week that's gonna be issued not solely going to be confined to issues of hacking, but also get into the dimension of this dissemination of fake news? Will that be one of the subject matters covered?

CLAPPER: Without preempting the report, we will describe the -- the full range of activities that the Russians undertook.

KAINE: I think that is incredibly important.

You know, I had a little role in this election. I was along for the ride for 105 days and was the subject of a couple of fake news stories. And it was interesting.

There were at least three that the mainstream media didn't cover because they were so incredible that like, why would they? But I looked at one of the stories that had been shared 800,000 times.

KAINE: And when I see an administration who is put in place as the proposed national security adviser, someone who traffics in these fake news stories and re-tweets them and shares them, who betrays a sense of either gullibility or malice that would kind of be -- that these are stories that most fourth graders would find incredible that a national security adviser would find them believable enough to share them causes me great concern.

Second, go back to Joe Dunford, he talked about Russia as a potential adversary because they had -- they had capacity and they had intent. With respect to our cyber, I think we have capacity.

But I think what we've shown is we haven't yet developed an intent about how, when, why, whether we're gonna use the capacity we have. So if we're gonna shore up our cyber defense, if I could just one word, do you think what we really need to shore up is our capacity or do we need to shore up our intent?

CLAPPER: Well, as -- as we look at foreign adversaries, that is always the issue is capability and intent. And certainly, with the indication to Russians, they do pose an existential threat to the United States.

And I -- I agree with Chairman Dunford on that. It's probably not our place and at least my place in the intelligence community to do an assessment of our intent. That's someone else's place, not mine.

MCCAIN: Senator Shaheen?

SHAHEEN: Thank you, Mr. Chairman and Senator Reed for holding this hearing and thank you all very much for testifying this morning and for your service to the country.

Dr. Robert Kagan testified before this committee last December, with respect to Russia. And at that time, there was less information known to the public about what had happened in their interference in the elections.

But one of the things he pointed out was that Russia is looking at interference in elections, whether that be cyber or otherwise the -- the whole messaging piece that you discussed with Senator Heinrich, as another strategy, along with their military action and economic and other diplomatic methods, to undermine Western values, our Euro-Atlantic alliance and the very democracies that make up that alliance.

Is that something that you agree with, Director Clapper?

CLAPPER: Yes, that's clearly a theme, it's certainly something that the Russians are pushing in messaging in Europe. They would very much like to drive wedges between us and Western Europe, the alliances there and between and among the countries in -- in Europe.

SHAHEEN: And I assume that there's agreement on the panel. Does anybody disagree with that?

So one of the things that I think has emerged, as I've listened to this discussion is that we don't have a strategy to respond to that kind of an effort. We don't have a strategy that's been testified with respect to cyber, but a broader strategy around messaging, around how to respond to that kind of activity. Do you agree with that?

CLAPPER: I think we -- I'm speaking personally...

SHAHEEN: Sure.

(CROSSTALK)

CLAPPER: ... institutional response and as I commented earlier to Senator McCain, I do think we -- we need a U.S. information agency on steroids, that deals with the totality of the information realm and who mount a -- in all forums and to include social media.

SHAHEEN: Can -- can I -- I'm sorry to interrupt. But can I just ask, why do you believe that hasn't happened?

Director Clapper, Admiral Rogers?

CLAPPER: I -- for my part, I -- I don't know why it hasn't. I can't answer that.

SHAHEEN: Admiral Rogers?

ROGERS: From my perspective in part because I don't think we've come yet to a full recognition of the idea that we have to gonna try to do something fundamentally different. I think we still continue to try -- to try to do some of the same traditional things we've done and expecting to do the same thing over and over again, yet achieve a different result.

I don't necessarily think...

SHAHEEN: No that's the definition of crazy, I think we've determined that.

Secretary Lettre?

LETTRE: I would just add that in this area, the capability and intent framework is -- is useful to think about. I think it is only in the last few years that we have seen adversaries with true intents to use propaganda and the ability to reach out as terrorists are doing or try to incite.

And match that up with the tremendous power that social media tools allow to make that easy and simple and effective and broadly applicable.

SHAHEEN: So, given that this is a strategy, and given that it's aimed not just at the United States, particularly with respect to interference in our elections, but at Western Europe and Eastern Europe, for that matter, is there an effort under way to work with our allies through NATO or otherwise?

I've been to the cybersecurity center in Estonia. But there didn't seem to be a NATO agreement that this was something that we should be working on together to respond to. So is this an effort that's under way?

LETTRE: Just speaking from my lens on things, there's a lot of interest in doing that and doing it more effectively and more comprehensively. But we have not cracked the code on doing it effectively yet. And so we need to keep the pressure on ourselves and our NATO allies who are like-minded in this regard to keep improving our approach.

CLAPPER: And it's also got to be much broader than just cyber.

SHAHEEN: Thank you.

Director Clapper, my time is almost up, but before you go, since this is the last opportunity we will have to hear from you, can I just ask you: Do you think that the DNI needs reform?

CLAPPER: Well, I -- there's always room for improvement. You know, I would never say that this is the ultimate. I do think it would be useful, though, if we're going to reform or change the DNI or change CIA that some attention be given to, in our case, the legislative underpinnings that established the DNI in the first place, and then have added additional functions and responsibilities over the years -- that Congress has added to our kitbag of duties.

So -- but to say that, you know, we can't -- there's not room for improvement, I'd never suggest that.

SHAHEEN: I appreciate that, and I certainly agree with you. I think that if there's going to be this kind of major reform, hopefully both legislators and others who have been engaged in the intelligence community will be part of that effort.

Thank you.

CLAPPER: I certainly agree that Congress, no pun intended, gets a vote here, I think.

SHAHEEN: Thank you.

MCCAIN: I know that our time is expired, and I apologize to our new members that we won't have time because you have to go. But maybe, Director Clapper, since this may be hopefully your last appearance, do you have any reflections that you'd like to provide us with, particularly the role of Congress or the lack of role of Congress in your years of experience?

CLAPPER: I'll have to be careful here.

(LAUGHTER)

MCCAIN: I don't think you have to be.

CLAPPER: I -- I was -- I was around in the intelligence community when the oversight committees were first established, and have watched them and experienced them ever since. Congress does have clearly an extremely important role to play whe

From: (b) (6)
To: [CS&C External Affairs](#); [NPPD_OPA_FO](#); [Schneck, Dr. Phyllis](#)
Cc: (b) (6); [CS&C External Affairs](#); (b) (6); [DUSCyber](#); (b) (6);
[CIR](#); [CS&C EXEC SEC](#); [NPPDExecSec](#); (b) (6); [NCCIC_Production](#); (b) (6);
(b) (6); [ASCyber](#); [OEC Outreach](#)
Subject: CS&C Daily Clips
Date: Tuesday, December 13, 2016 9:03:46 AM

CS&C Daily Clips December 13, 2016

[DHS: Georgia incident was legitimate work, not a hack \(12/12\) – Fedscoop](#)

Someone used the department's security network to conduct legitimate business, DHS said. According to DHS, someone on the federal department's security network was conducting legitimate business on the state office's website, verifying a professional license administered by the state. The state office manages information about corporate licenses and certificates on its website.

[Hack of Quest Diagnostics App Exposes Data of 34,000 Patients \(12/12\) – New York Times](#)

An "unauthorized third party" gained access to names, dates of birth, lab results and, in some cases, telephone numbers on Nov. 26 through a mobile health app that gives patients access to lab results and other information, [according to the company](#), Quest Diagnostics, which is based in Madison, N.J.

[3 takeaways from the FITARA 3.0 hearing \(12/12\) – Federal News Radio](#)

The State and Homeland Security departments' chief information officers offered a better understanding of their progress in reforming IT in their respective agencies.

[Unplug Your Easily Hijacked Netgear Routers Pronto \(12/12\) – Fortune](#)

"Exploiting this vulnerability is trivial," US-CERT, a cybersecurity unit within the Department of Homeland Security, [warned in a bulletin](#) on Friday. The note urged consumers to "strongly consider discontinuing use of affected devices until a fix is made available."

[Preventing not-so-happy holidays fraud \(12/12\) – The Detroit News](#)

The most common ways criminals can access your personal and financial information, according to the U.S. Computer Emergency Readiness Team, which is part of the Department of Homeland Security, are creating fraudulent sites and email messages, intercepting insecure transactions and targeting vulnerable computers.

[Republican leaders join outrage at Russia, will investigate hacks \(12/12\) – USA Today](#)

Republican congressional leaders said Monday that key committees will investigate CIA allegations that Russia deployed hackers to disrupt the American presidential election to help President-elect Donald Trump and hurt Democrat Hillary Clinton.

[Young people targeted in world-wide cyber crime crackdown \(12/12\) – News-PressNow.com](#)

Law enforcement agencies from 13 countries, including the United States, ran a coordinated crackdown earlier this month on young people who are committing cyber-attack tools around the world.

Click [here](#) for previous CS&C EA Daily Clips

From: (b) (6)
To: [CS&C External Affairs](#); [NPPD_OPA_FO](#); [Schneck, Dr. Phyllis](#)
Cc: (b) (6); [CS&C External Affairs](#); (b) (6); [DUSCyber](#); (b) (6);
(b) (6); [CS&C EXEC SEC](#); [NPPDExecSec](#); (b) (6); [NCCIC_Production](#); (b) (6);
(b) (6); [ASCyber](#); [O&C Outreach](#)
Subject: CS&C Daily Clips
Date: Friday, December 30, 2016 9:41:00 AM

CS&C Daily Clips
December 30, 2016

[Yes, pacemakers can get hacked](#) (12/29) – New York Post

The Food and Drug Administration this week published guidelines to help medical manufacturers prevent hackers from breaking into implantable devices that operate with the help of cloud-based networks.

[Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'](#) (12/29) – Reuters

Hackers have targeted Ukrainian state institutions about 6,500 times in the past two months, including incidents that showed Russian security services were waging a cyberwar against the country, President Petro Poroshenko said on Thursday.

-

[Obama Sanctions Russia for Election Hacking](#) (12/29) – Nextgov

Thursday's order also expelled 35 diplomats, who officials said were covert intelligence agents, from the Russian embassy in Washington and blocked Russian access to two Russian government-owned facilities in New York and Maryland they said were being used for intelligence operations.

[Trump: It's time 'to move on' from claims of Russian interference in election](#) (12/29) – Politico

The president-elect also pledges to meet with leaders of the intelligence community 'to be updated on the facts.'

[Russia 'Grizzly Steppe' Hacking Started Simply, U.S. Says](#) (12/30) – Bloomberg

U.S. intelligence agencies say that was the modest start of "Grizzly Steppe," their name for what they say developed into a far-reaching Russian operation to interfere with this year's presidential election.

-

Click [here](#) for previous CS&C EA Daily Clips

From: (b) (6)
To: NICC; OECOutreach; Events, US-Cert; NCC; NCCIC; NCCIC - USCERT; (b) (6)

Subject: FW: CS&C Daily Clips
Date: Tuesday, December 13, 2016 9:39:51 AM

CS&C Daily Clips December 13, 2016

DHS: Georgia incident was legitimate work, not a hack (12/12) – Fedscoop

Someone used the department's security network to conduct legitimate business, DHS said. According to DHS, someone on the federal department's security network was conducting legitimate business on the state office's website, verifying a professional license administered by the state. The state office manages information about corporate licenses and certificates on its website.

Hack of Quest Diagnostics App Exposes Data of 34,000 Patients (12/12) – New York Times

An "unauthorized third party" gained access to names, dates of birth, lab results and, in some cases, telephone numbers on Nov. 26 through a mobile health app that gives patients access to lab results and other information, according to the company, Quest Diagnostics, which is based in Madison, N.J.

3 takeaways from the FITARA 3.0 hearing (12/12) – Federal News Radio

The State and Homeland Security departments' chief information officers offered a better understanding of their progress in reforming IT in their respective agencies.

Unplug Your Easily Hijacked Netgear Routers Pronto (12/12) – Fortune

"Exploiting this vulnerability is trivial," US-CERT, a cybersecurity unit within the Department of Homeland Security, warned in a bulletin on Friday. The note urged consumers to "strongly consider discontinuing use of affected devices until a fix is made available."

Preventing not-so-happy holidays fraud (12/12) – The Detroit News

The most common ways criminals can access your personal and financial information, according to the U.S. Computer Emergency Readiness Team, which is part of the Department of Homeland Security, are creating fraudulent sites and email messages, intercepting insecure transactions and targeting vulnerable computers.

[Republican leaders join outrage at Russia, will investigate hacks \(12/12\) – USA Today](#)

Republican congressional leaders said Monday that key committees will investigate CIA allegations that Russia deployed hackers to disrupt the American presidential election to help President-elect Donald Trump and hurt Democrat Hillary Clinton.

[Young people targeted in world-wide cyber crime crackdown \(12/12\) – News-PressNow.com](#)

Law enforcement agencies from 13 countries, including the United States, ran a coordinated crackdown earlier this month on young people who are committing cyber-attack tools around the world.

Click [here](#) for previous CS&C EA Daily Clips

From: (b) (6)
To: NICC; OECOutreach; Events, US-Cert; NCC; NCCIC; NCCIC - USCERT; (b) (6)

Subject: FW: CS&C Daily Clips
Date: Tuesday, December 13, 2016 9:38:52 AM

CS&C Daily Clips December 13, 2016

DHS: Georgia incident was legitimate work, not a hack (12/12) – Fedscoop

Someone used the department's security network to conduct legitimate business, DHS said. According to DHS, someone on the federal department's security network was conducting legitimate business on the state office's website, verifying a professional license administered by the state. The state office manages information about corporate licenses and certificates on its website.

Hack of Quest Diagnostics App Exposes Data of 34,000 Patients (12/12) – New York Times

An "unauthorized third party" gained access to names, dates of birth, lab results and, in some cases, telephone numbers on Nov. 26 through a mobile health app that gives patients access to lab results and other information, according to the company, Quest Diagnostics, which is based in Madison, N.J.

3 takeaways from the FITARA 3.0 hearing (12/12) – Federal News Radio

The State and Homeland Security departments' chief information officers offered a better understanding of their progress in reforming IT in their respective agencies.

Unplug Your Easily Hijacked Netgear Routers Pronto (12/12) – Fortune

"Exploiting this vulnerability is trivial," US-CERT, a cybersecurity unit within the Department of Homeland Security, warned in a bulletin on Friday. The note urged consumers to "strongly consider discontinuing use of affected devices until a fix is made available."

Preventing not-so-happy holidays fraud (12/12) – The Detroit News

The most common ways criminals can access your personal and financial information, according to the U.S. Computer Emergency Readiness Team, which is part of the Department of Homeland Security, are creating fraudulent sites and email messages, intercepting insecure transactions and targeting vulnerable computers.

[Republican leaders join outrage at Russia, will investigate hacks \(12/12\) – USA Today](#)

Republican congressional leaders said Monday that key committees will investigate CIA allegations that Russia deployed hackers to disrupt the American presidential election to help President-elect Donald Trump and hurt Democrat Hillary Clinton.

[Young people targeted in world-wide cyber crime crackdown \(12/12\) – News-PressNow.com](#)

Law enforcement agencies from 13 countries, including the United States, ran a coordinated crackdown earlier this month on young people who are committing cyber-attack tools around the world.

Click [here](#) for previous CS&C EA Daily Clips

From: (b) (6)
To: OECOutreach; NICC; Events, US-Cert; NCC; NCCIC; NCCIC - USCERT; (b) (6)

Subject: FW: CS&C Daily Clips
Date: Friday, December 30, 2016 12:44:55 PM

CS&C Daily Clips
December 30, 2016

[Yes, pacemakers can get hacked](#) (12/29) – New York Post

The Food and Drug Administration this week published guidelines to help medical manufacturers prevent hackers from breaking into implantable devices that operate with the help of cloud-based networks.

[Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'](#) (12/29) – Reuters

Hackers have targeted Ukrainian state institutions about 6,500 times in the past two months, including incidents that showed Russian security services were waging a cyberwar against the country, President Petro Poroshenko said on Thursday.

-

[Obama Sanctions Russia for Election Hacking](#) (12/29) – Nextgov

Thursday's order also expelled 35 diplomats, who officials said were covert intelligence agents, from the Russian embassy in Washington and blocked Russian access to two Russian government-owned facilities in New York and Maryland they said were being used for intelligence operations.

[Trump: It's time 'to move on' from claims of Russian interference in election](#) (12/29) – Politico

The president-elect also pledges to meet with leaders of the intelligence community 'to be updated on the facts.'

[Russia 'Grizzly Steppe' Hacking Started Simply, U.S. Says](#) (12/30) – Bloomberg

U.S. intelligence agencies say that was the modest start of "Grizzly Steppe," their name for what they say developed into a far-reaching Russian operation to interfere with this year's presidential election.

-

Click [here](#) for previous CS&C EA Daily Clips

From: (b) (6)
To: OECOutreach; NICC; Events, US-Cert; NCC; NCCIC; NCCIC - USCERT; (b) (6)

Subject: FW: CS&C Daily Clips
Date: Friday, December 30, 2016 12:46:16 PM

CS&C Daily Clips
December 30, 2016

[Yes, pacemakers can get hacked](#) (12/29) – New York Post

The Food and Drug Administration this week published guidelines to help medical manufacturers prevent hackers from breaking into implantable devices that operate with the help of cloud-based networks.

[Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'](#) (12/29) – Reuters

Hackers have targeted Ukrainian state institutions about 6,500 times in the past two months, including incidents that showed Russian security services were waging a cyberwar against the country, President Petro Poroshenko said on Thursday.

-

[Obama Sanctions Russia for Election Hacking](#) (12/29) – Nextgov

Thursday's order also expelled 35 diplomats, who officials said were covert intelligence agents, from the Russian embassy in Washington and blocked Russian access to two Russian government-owned facilities in New York and Maryland they said were being used for intelligence operations.

[Trump: It's time 'to move on' from claims of Russian interference in election](#) (12/29) – Politico

The president-elect also pledges to meet with leaders of the intelligence community 'to be updated on the facts.'

[Russia 'Grizzly Steppe' Hacking Started Simply, U.S. Says](#) (12/30) – Bloomberg

U.S. intelligence agencies say that was the modest start of "Grizzly Steppe," their name for what they say developed into a far-reaching Russian operation to interfere with this year's presidential election.

-

Click [here](#) for previous CS&C EA Daily Clips

SPEAKER REQUEST FORM
U.S. Department of Homeland Security (DHS)
Office of Cybersecurity and Communications (CS&C) Speakers Bureau

Deadline for Acceptance:	March 15, 2016
Event Title:	NACD Global Board Leaders' Summit
Speech Date:	Sept. 19 or Sept. 20
Speech Time & Duration:	Sept. 20 10-10:45 a.m. Alternate times: Sept. 19: 5:15-6:15 p.m.; OR 11-11:50 a.m.
Speaker Requested:	Dr. Phyllis Schneck
Pursue a Surrogate if Requested Speaker is Not Available:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Event Location:	Marriott Marquis Washington, DC 901 Massachusetts Avenue NW Washington, DC 20001
Open Press/Closed Press:	<input checked="" type="checkbox"/> Open Press <input type="checkbox"/> Closed Press Typically Bloomberg, WSJ
Will the Event Be Webcast, Recorded, or Transcribed?:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Video for NACD purposes
Purpose:	This is the largest director forum in the world, where the greatest minds in governance convene to take on the largest issues facing today's boardrooms and collectively discover the future of exemplary board leadership.
Is the Event For Profit or Not for Profit?:	<input type="checkbox"/> For Profit <input checked="" type="checkbox"/> Not For Profit
Is There a Fee for the Speaker to Attend?:	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No N/A
Offer of Payment/Reimbursement:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No negotiable
Speech Topic:	Cybersecurity
Presentation Format:	<input checked="" type="checkbox"/> Keynote <input type="checkbox"/> Non-Keynote Speech <input type="checkbox"/> Panel Discussion <input type="checkbox"/> Program Brief <input type="checkbox"/> Other
Dress Code:	Business attire
Will There Be A Question & Answer Period?:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No negotiable
Audience:	<ul style="list-style-type: none">• NACD Members across the 50 states and 16 different countries across the globe• Chairmen and Directors of top Public, Private, and Not-for-Profit Boards• More than 20 percent of the Fortune 1000• Chairs of Audit, Compensation, Nominating & Governance, and Risk Committees• Corporate Directors and Governance Experts concerned with the advancement of exemplary board leadership in their

SPEAKER REQUEST FORM

boardroom and in boardrooms worldwide

Event Web Site:	https://www.nacdonline.org/Summit
Event Sponsor:	NACD works with a number of strategic partners on this event. For reference, review the 2015 partners (scroll to the bottom of the webpage): https://www.nacdonline.org/Conference/index.cfm
Relationship to DHS CS&C:	Yes, we have worked together to produce a cybersecurity handbook.
Event Agenda:	The four-day agenda has not been released to the public yet. Please review our 2015 agenda for reference: https://www.nacdonline.org/Conference/agenda.cfm
Honorable Guests Attending:	TBA
Federal, State or local Appointed or Elected officials attending:	N/A
Person to contact for speechwriting purposes:	Erin Essenmacher, Chief Programming Officer, 202-380-1896, eesenmacher@nacdonline.org
Day of Event Point of Contact:	Cheryl Martel, 202-280-2183, csmartel@nacdonline.org
Disclaimer/Release Form:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

FOR INTERNAL USE ONLY

Part of your projected travel? ☐ Yes ☐ No

Justification Statement: Outline the benefit of your attendance to the Department and how your attendance at this particular event furthers the mission of CS&C and NPPD.

Proposed Topic Please outline what you plan to discuss or present. Attach talking points or your presentation with this form.

Program Director Approval:

DHS directs event organizers to not list DHS speakers as “Invited” or “Attending” for any event promotional and marketing material, including but not limited to web sites, press releases, media advisories, flyers, programs, agendas, etc., without obtaining prior written DHS approval.

In the event that DHS approves the speaker’s participation in the event, the event organizer must obtain prior written approval from DHS for language to be used in any references to DHS speakers on all event materials.

Use of the DHS official seal is prohibited without prior written approval from DHS. Event organizers seeking to use the DHS Seal in any context must submit a written request to DHS that specifies in detail the exact use to be made of the seal. Any permission granted will apply only to the specific use outlined in the written request and is not construed as permission for any other use.

Please submit this form to: CSCEExternalAffairs@hq.dhs.gov

SPEAKER REQUEST FORM

(b) (6)

First Name	Last Name	Primary Title	Primary Company	Contact: Current Boards	LOCATION
------------	-----------	---------------	-----------------	-------------------------	----------

NACD PRESS LIST

AS OF 9/15/16

The Wall Street Journal

Atlantic Media

Thomas Reuters

MarketWatch

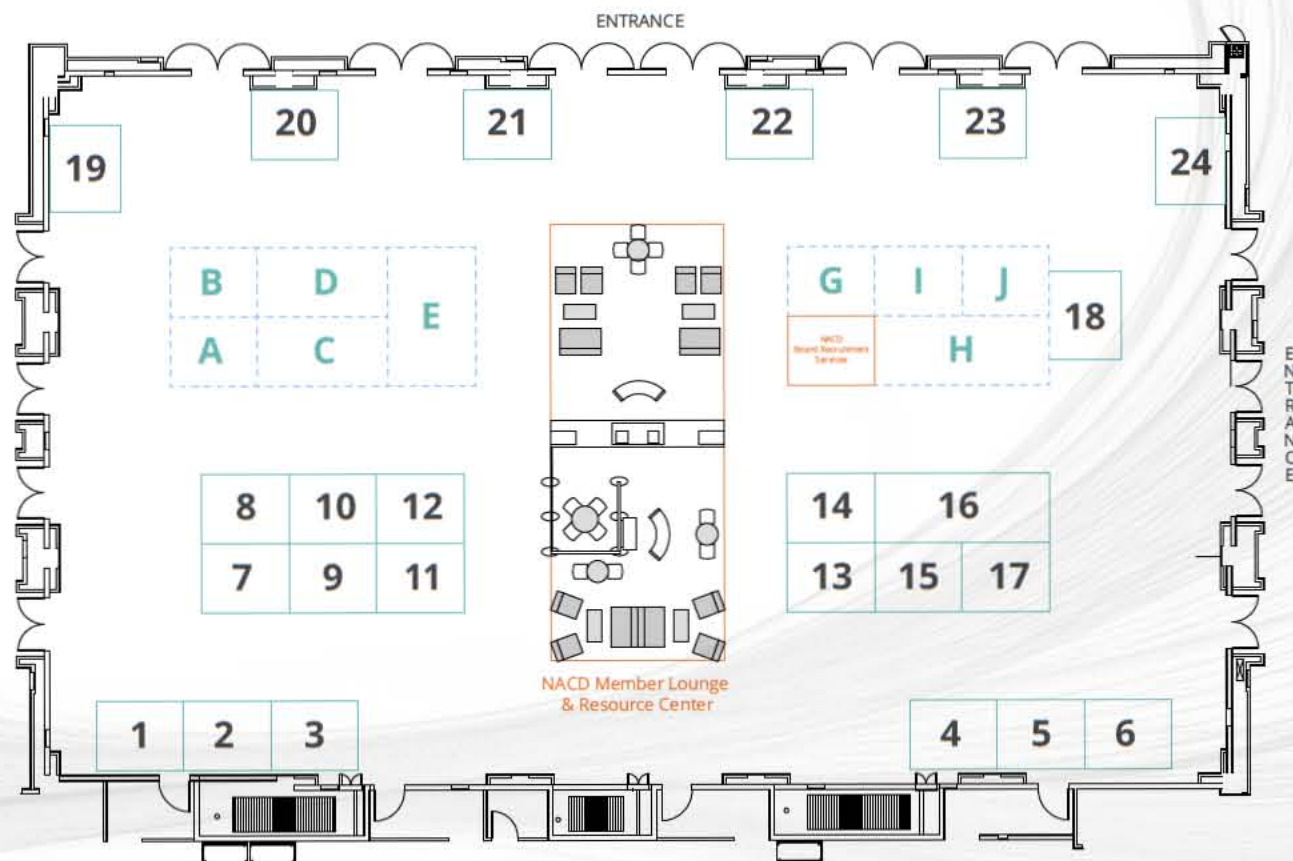
Bloomberg

NBC Universal Media LLC

AP Capital, Inc.

The Hill

Agenda



INNOVATION NATION & PARTNER SHOWCASE LIBERTY BALLROOM

PARTNER SHOWCASE

Company

Baker Tilly Virchow Krause, LLP
BDO USA, LLP
Broadridge Financial Solutions, Inc.
Crowe Horwath LLP
CyberVista
Dechert LLP
Deloitte LLP
Diligent Corporation
EVA Dimensions LLC
EY
Enlight Research
Grant Thornton LLP
IBM Security
The Institute of Internal Auditors
Korn Ferry
KPMG LLP
Meridian Compensation Partners, LLC
Minority Corporate Counsel Association
NASDAQ
Pearl Meyer
Rapid7
RSM US LLP
SecureWorks
Vinson & Elkins LLP

Booth

21
13
15
10
1
23
5
11
2
3
20
19
18
7
6
16
12
14
4
22
17
24
8
9

INNOVATION NATION

AeroVista Innovations
Chapul
cove
Dancing With the Start-Ups
Department of Transportation
IBM
KPMG LLP
Powerlytics
PureWine, Inc.

I
A
H
C
J
D
E
B
G

UNIQUE EXPERIENCES FOR EVERY DIRECTOR NEED

The profession of directorship is rapidly changing—and so is the environment we're operating in. While the topics essential to shaping board leadership will be covered by keynotes and general sessions throughout the 2016 Summit agenda, each Unique Experience will offer a new format for learning—and a new way of thinking. Take it all in, engage, and be inspired to think differently.



ASK THE EXPERTS

Locations vary. Check agenda.

MONDAY, SEPT. 19 | 2:00 PM – 3:15 PM

We've gathered leading minds from across the country to share their perspectives on a variety of key governance topics. Challenge their answers and seek proof. Cause a ruckus. This is your chance to create intellectual havoc and leave everyone smarter, wiser, and better prepared.



CONVERGENCE LAB

Locations vary. Check agenda.

MONDAY, SEPT. 19

11:00 AM | 2:00 PM | 3:45 PM

Think of these as the "lightning rounds" of the Summit. Three short keynote speeches—all with a different take on a singular topic—will give you at least one new perspective on an important issue shaping your boardroom agenda. Put on your thinking cap. We'll provide the electricity.



DANCING WITH THE START-UPS

Independence Ballroom (M4)

SUNDAY, SEPT. 18 | 3:30 PM – 5:00 PM

This is a fast-paced, Shark Tank-style challenge where promising start-ups have minutes to showcase their company's vision and a panel of expert judges selects a winner. See what goes into a successful pitch and hear open feedback from the judges—directors themselves, innovation experts, and prominent executives.



DIVERSITY SYMPOSIUM

Independence Ballroom (M4)

SATURDAY, SEPT. 17 | 12:30 PM – 4:45 PM

Join us for a thought-provoking afternoon of programming dedicated to discussing the realities of unconscious bias, the impact diversity has on your business, and when board refreshment is necessary.



INNOVATION NATION

Liberty Ballroom

SUNDAY, SEPT. 18 | 2:30 PM – 5:00 PM

MONDAY, SEPT. 19 | 6:45 AM – 5:00 PM

Back for its second year, Innovation Nation showcases cutting-edge and disruptive technologies that boards should have on their radar. Experience technologies that will change our future.



MEET-UPS

Locations vary. Check agenda.

MONDAY, SEPT. 19 | 3:45 PM – 4:45 PM

Looking to meet directors who are facing the same challenges that bedevil you? Even better, would you like to hear their solutions and expand the talent pipeline for your board? These informal gatherings are designed to help you make new connections in a more intimate setting. Choose your Meet-Up by board role or company type (see agenda).



PEER EXCHANGE

Locations vary. Check agenda.

SUNDAY, SEPT. 18 | 3:30 PM – 4:45 PM

These small group discussions create an intimate setting to showcase leading practices and gain new perspectives, and they are specifically designed to help you make new connections. Choose your Peer Exchange by industry (see agenda).



POWER BREAKFASTS

Locations vary. Check agenda.

MONDAY, SEPT. 19 | 7:00 AM – 8:00 AM

TUESDAY, SEPT. 20 | 7:00 AM – 8:00 AM

Set your alarms—these morning sessions are worth waking up early for. Start your day with an interactive discussion on key issues facing the governance community. Topics range from economic trends to board composition to shareholder activism. You bring your expertise and questions. We'll provide the thought leaders and the coffee.



THINK TANK

Locations vary. Check agenda.

MONDAY, SEPT. 19 | 11:00 AM | 2:00 PM | 3:45 PM

If you came to talk about pay ratio or auditor independence, we have a place for you... but this isn't it! These sessions are meant to challenge your thinking, encourage lateral shifts, and deliver new perspectives on emerging issues both inside and outside the governance arena. Check your preconceived notions at the door and take a deep dive into a big tank.

SATURDAY SEPTEMBER 17, 2016
9:00 AM – 7:00 PM
SUMMIT REGISTRATION AND INFORMATION Independence Ballroom Foyer (M4)
12:30 PM – 4:45 PM
DIVERSITY SYMPOSIUM Independence Ballroom (M4)
12:30 PM – 12:35 PM
PROGRAM WELCOME AND INTRODUCTIONS Independence Ballroom (M4)
12:35 PM – 1:20 PM
BREAKING THROUGH UNCONSCIOUS BIAS Independence Ballroom (M4)
1:20 PM – 1:30 PM
NETWORKING BREAK
1:30 PM – 2:15 PM
UNLOCKING INNOVATION THROUGH DIVERSITY Independence Ballroom (M4)
2:15 PM – 2:30 PM
NETWORKING BREAK
2:30 PM – 3:00 PM
MEGATRENDS Independence Ballroom (M4)
3:00 PM – 3:45 PM
THE 21ST CENTURY DIRECTOR Independence Ballroom (M4)
3:45 PM – 4:00 PM
NETWORKING BREAK
4:00 PM – 4:45 PM
OPERATIONALIZING THE HIGH-PERFORMANCE BOARD Independence Ballroom (M4)
4:45 PM – 6:00 PM
NETWORKING RECEPTION Capitol/Congress (M4)
6:30 PM – 8:00 PM
INNOVATION NATION SNEAK-PEEK (NACD FELLOWS AND CHAPTER LEADERS ONLY) Liberty Ballroom (M4)
SUNDAY SEPTEMBER 18, 2016
7:00 AM – 7:30 PM
SUMMIT REGISTRATION AND INFORMATION Independence Ballroom Foyer (M4)
8:15 AM – 9:00 AM
GETTING THE MOST FROM YOUR SUMMIT EXPERIENCE Shaw/LeDroit Park (M3)
9:30 AM – 2:30 PM
BOARD COMMITTEE FORUMS:

» Compensation Salon 12/13 (M2)
» Nominating and Governance Independence E-F (M4)
» Nonprofit Monument (M4)
» Private Company Archives (M4)
» Small-Cap Supreme Court (M4)
» Strategy and Risk Capitol/Congress (M4)
2:30 PM – 5:00 PM
INNOVATION NATION AND PARTNER SHOWCASE OPEN Liberty Ballroom (M4)
3:30 PM – 5:00 PM
DANCING WITH THE START-UPS Independence Ballroom (M4)
» BoostUp
» Disease Diagnostics Group
» Geostellar Inc.
» Maven
» Mercari's
» Plaid
» Simple Energy
» Tank Utility
» Vital Vio
» Wealthminder
» Welthh
» Zeel
3:30 PM – 4:45 PM
SMALL GROUP PEER EXCHANGE
» Financial services/insurance Judiciary Square (M3)
» Energy Mount Vernon (M3)
» Healthcare LEnfant Plaza Room (M3)
» Consumer goods Gallery Place (M3)
» Manufacturing Eastern Market (M3)
» Technology Farragut North (M3)
5:15 PM – 5:45 PM
OPEN GENERAL SESSION AND CHAIRS REMARKS Marquis Ballroom (M2)
5:45 PM – 6:15 PM
OPENING KEYNOTE Marquis Ballroom (M2)
6:15 PM – 7:00 PM
IN CONVERSATION WITH... RON WILLIAMS Marquis Ballroom (M2)

7:00 PM – 8:30 PM
WELCOME RECEPTION AND PARTNER SHOWCASE Liberty Ballroom (M4)
MONDAY SEPTEMBER 19, 2016
6:30 AM – 6:00 PM
SUMMIT REGISTRATION AND INFORMATION Independence Ballroom Foyer (M4)
6:45 AM – 5:00 PM
INNOVATION NATION AND PARTNER SHOWCASE OPEN Liberty Ballroom (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: 2017 ECONOMIC FORECAST: CLOUDY WITH A CHANCE OF DISRUPTION Shaw/LeDroit Park (M3)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: SMALL- AND MID-CAP COMPANY AUDIT QUALITY Independence A-D (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: HOW WELL IS YOUR COMPANY REALLY DOING? Archives (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: INNOVATION GAME CHANGERS Capitol/Congress (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: MEGATRENDS, STRATEGY, AND THE BOARD OF THE FUTURE Independence E-H (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: RESPONDING TO BUSINESS DISRUPTION Chinatown (M3)
8:15 AM – 8:30 AM
CEOs WELCOME Marquis Ballroom (M2)
8:30 AM – 9:15 AM
KEYNOTE Marquis Ballroom (M2)
9:15 AM – 9:30 AM
NETWORKING BREAK
9:30 AM – 10:15 AM
ECONOMICS, UNCERTAINTY, AND THE 2016 ELECTION Marquis Ballroom (M2)
10:15 AM – 10:45 AM
SHORT TAKES ON BIG IDEAS Marquis Ballroom (M2)
11:00 AM – 12:00 PM <i>concurrent session</i>
AUDIT HOT TOPICS Independence A-D (M4)
11:00 AM – 12:00 PM <i>concurrent session</i>
BALANCING GROWTH AND RISK IN THE AGE OF OPEN INNOVATION Monument (M4)

11:00 AM – 12:00 PM <i>concurrent session</i>
CORPORATE TURNAROUNDS Shaw/LeDroit Park (M3)
11:00 AM – 12:00 PM <i>concurrent session</i>
DISRUPTIVE TIMES CALL FOR EVOLVING STRATEGIES Judiciary Square (M3)
11:00 AM – 12:00 PM <i>concurrent session</i>
GLOBALIZATION OF GOVERNANCE: IMPLICATIONS FOR COMP AND NOM/GOV COMMITTEES Chinatown (M3)
11:00 AM – 12:00 PM <i>concurrent session</i>
GOVERNING COMPLEXITY Supreme Court (M4)
11:00 AM – 12:00 PM <i>concurrent session</i>
INNOVATING SUSTAINABILITY Union Station (M3)
11:00 AM – 12:00 PM <i>concurrent session</i>
ACTIVISTS AND THE RISE OF THE HIGHLY ENGAGED SHAREOWNER Independence E-H (M4)
11:00 AM – 12:00 PM <i>concurrent session</i>
IN CONVERSATION WITH... GENERAL MICHAEL HAYDEN Salon 12/13 (M2)
11:00 AM – 12:00 PM <i>concurrent session</i>
SUCCESSFUL SUCCESSION PLANNING Archives (M4)
11:00 AM – 12:00 PM <i>concurrent session</i>
CONVERGENCE LAB: GLOBAL/COMPETITION Capitol/Congress (M4)
11:00 AM – 12:00 PM <i>concurrent session</i>
THINK TANK: REBOOTING CAPITALISM Mount Vernon Square (M3)
12:00 PM – 1:45 PM
LUNCH KEYNOTE: FOOLPROOF: HOW SAFETY CREATES DANGER Marquis Ballroom (M2)
2:00 PM – 3:30 PM <i>concurrent session</i>
WORKSHOP: COMMUNICATION AND INCLUSION DYNAMICS IN THE BOARDROOM Monument (M4)
2:00 PM – 3:30 PM <i>concurrent session</i>
WORKSHOP: EFFECTIVE IT GOVERNANCE Shaw/LeDroit Park (M3)
2:00 PM – 3:30 PM <i>concurrent session</i>
WORKSHOP: LANDING YOUR NEXT BOARD SEAT Independence A-D (M4)
2:00 PM – 3:30 PM <i>concurrent session</i>
WORKSHOP: AUDITING SOCIAL MEDIA Independence E-H (M4)
2:00 PM – 3:15 PM <i>concurrent session</i>
ASK THE EXPERTS: CYBER RISK Salon 12/13 (M2)

2:00 PM – 3:15 PM <i>concurrent session</i>
ASK THE EXPERTS: SHAREHOLDER ACTIVISM Archives (M4)
2:00 PM – 3:15 PM <i>concurrent session</i>
ASK THE EXPERTS: THE BOARD'S ROLE IN VALUE CREATION Mount Vernon Square (M3)
2:00 PM – 3:00 PM <i>concurrent session</i>
WHY ARE COMPANIES CHANGING THE DESIGN OF EXECUTIVE-PAY PROGRAMS? Supreme Court (M4)
2:00 PM – 3:00 PM <i>concurrent session</i>
PRIVATE COMPANY M&A DEALS Union Station (M3)
2:00 PM – 3:00 PM <i>concurrent session</i>
CONVERGENCE LAB: HUMAN/CAPITAL Capitol/Congress (M4)
2:00 PM – 3:00 PM <i>concurrent session</i>
THINK TANK: THE POWER OF INTROVERTS Chinatown (M3)
3:00 PM – 3:45 PM
NETWORKING BREAK
3:45 PM – 4:45 PM <i>concurrent session</i>
CORPORATE RESILIENCY Independence A-D (M4)
3:45 PM – 4:45 PM <i>concurrent session</i>
DRIVING STRATEGY THROUGH COMPENSATION Shaw/LeDroit Park (M3)
3:45 PM – 4:45 PM <i>concurrent session</i>
FUTURE OF PRIVACY Independence E-H (M4)
3:45 PM – 4:45 PM <i>concurrent session</i>
THE GLOBAL DIRECTOR Chinatown (M3)
3:45 PM – 4:45 PM <i>concurrent session</i>
CONVERGENCE LAB: RISK/INNOVATION Archives (M4)
3:45 PM – 4:45 PM <i>concurrent session</i>
MEET-UP
» Energy Supreme Court (M4)
» Financial Services Salon 12/13 (M2)
» Healthcare Mount Vernon Square (M3)
» Lead Director Monument (M4)
» Private/Family Companies Union Station (M3)
3:45 PM – 4:45 PM <i>concurrent session</i>
THINK TANK: A LESSON IN INNOVATION FROM THE UNDERGROUND RAILROAD Capitol/Congress (M4)
5:00 PM – 5:30 PM
SHORT TAKES ON BIG IDEAS Marquis Ballroom (M2)

5:30 PM – 6:15 PM
IN CONVERSATION WITH... MICHELLE CROSBY Marquis Ballroom (M2)
6:30 PM – 8:30 PM
NETWORKING RECEPTION: THE TASTE OF WASHINGTON Mezzanine Foyer (2nd)
TUESDAY SEPTEMBER 20, 2016
6:30 AM – 12:00 PM
SUMMIT REGISTRATION AND INFORMATION Independence Ballroom Foyer (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
A TALENT-CENTERED APPROACH TO LONG-TERM VALUE CREATION Archives (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
THE FUTURE OF SEARCH Independence Ballroom (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: COMMUNICATING IN CRITICAL TIMES Capitol/Congress (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
POWER BREAKFAST: FAMILY BUSINESS: GOVERNING THROUGH COMPLEXITY AND CONFLICT Monument (M4)
7:00 AM – 8:00 AM <i>concurrent session</i>
ANATOMY OF A PARADIGM SHIFT: INNOVATING HEALTHCARE Salon 12/13 (M4)
8:15 AM – 8:45 AM
KEYNOTE: CYBERSECURITY Marquis Ballroom (M2)
8:45 AM – 9:15 AM
SHORT TAKES ON BIG IDEAS Marquis Ballroom (M2)
9:15 AM – 9:30 AM
NETWORKING BREAK
9:30 AM – 10:15 AM
KEYNOTE Marquis Ballroom (M2)
10:15 AM – 11:00 AM
HIGHER-AMBITION BOARDS Marquis Ballroom (M2)
11:00 AM – 11:15 AM
NETWORKING BREAK
11:15 AM – 12:00 PM
IN CONVERSATION WITH... SCOTT KUPOR Marquis Ballroom (M2)
12:00 PM
PROGRAM ADJOURNS Marquis Ballroom (M2)

Registration

Please proceed to the **M4 Level** of the Marriott Marquis to receive your Summit badge and program materials.

Session Information

Session: Keynote: Cybersecurity

Date/Time: Tuesday, September 20, 2016 | 8:15AM - 8:45AM

Room Location: Marquis Ballroom (M2 Level)

When and where should I arrive before my scheduled session?

- If your session is on the mainstage at the Marquis Ballroom (M2 Level), **please proceed to the Speaker Check-In area of the ballroom and arrive at least 30 minutes prior** to your session start time.
- If your session is in one of the breakout rooms at the M2/M3/M4 Levels, **please proceed to the AV table in your session room at least 20 minutes prior** to your session start time.

New This Year! - Speaker Lounge

A private lounge for speakers will be available on the M2 Level in room Salon 11. Snacks and beverages will be provided.

Dress Code Consideration for AV Requirements

Business attire is recommended. Please note that the majority of our Summit speakers will be provided lavalier microphones (*lapel microphones*) for their presentation. These microphones provide a greater degree of movement and can be very discreet, but require wires to be run to a transmitter worn by the user. Typically this transmitter is positioned around the waist. **Therefore it is extremely important that your attire have some form of waistband or belt to which the transmitter/battery pack can be attached.** Please do not put the transmitter and battery pack into a jacket pocket, as it disturbs the line of your clothes, and may cause interference. It is also preferred that you have a stiff lapel to attach the microphone to, as opposed to a soft silk collar, and refrain from wearing large pieces of jewellery, scarves, or watches/wearables with Bluetooth capability.

Need to Contact Us?

If you need to reach a staff member from the Education team during the Summit, please do not hesitate to contact us at one of the numbers/email addresses below:

Cheryl Martel, Senior Manager, Education Content: (412) 600-7044 | csmartel@nacdonline.org

Emily Toth, Assistant Programs Manager: (719) 445-6876 | etoth@nacdonline.org

Michael Kelly, Education Content Associate: (201) 741-2861 | mkelly@nacdonline.org

The subsequent 66 pages, (NPPD 001995 through NPPD 002060) are being withheld in their entirety pursuant to 5 U.S.C. § 552 (b)(4), (b)(5) and (b)(6).

NPPD 001995 – NPPD 002060