Battling Cybersecurity Threats: Role of Congressional Oversight

Online Panel Presented by

Levin Center at Wayne Law/Wayne Law Review

June 24, 2020

Battling Cybersecurity Threats: Role of Congressional Oversight

Panel Introduction

Moderator: Frederick Chang, Southern Methodist University

Panelists:

- Patrick Warren, U.S. Senate Permanent Subcommittee on Investigations
- Kimberly Breedon, Barry University School of Law, Chris Bryant, U. of Cincinnati
- M. Tia Johnson, Georgetown University Law Center
- Jonathan Lewallen, University of Tampa

Battling Cybersecurity Threats

Congressional Oversight is Challenging

- Testified in three separate Congressional hearings
- Speed of technological change
- Technological complexity
- Constantly evolving threat landscape

Senate Permanent Subcommittee on Investigations

PSI Jurisdiction

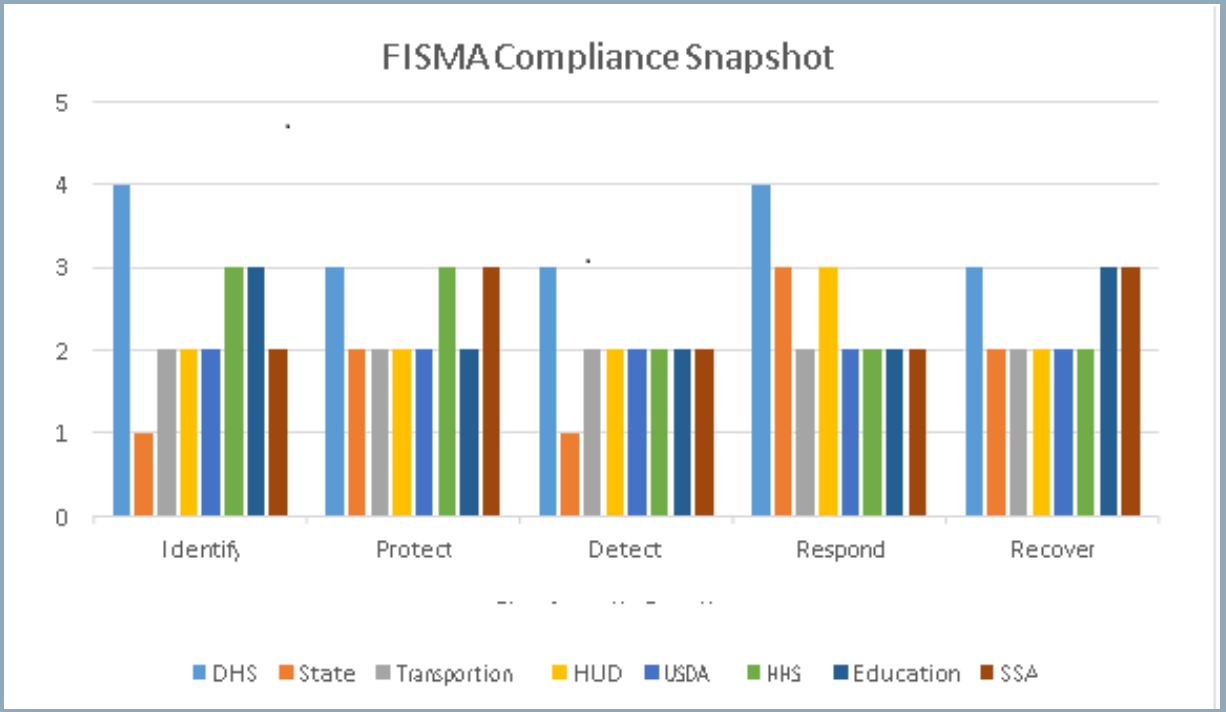
- The Permanent Subcommittee on Investigations is the Homeland Security and Governmental Affairs Committee's ("HSGAC") chief investigative subcommittee.
- PSI has the responsibility of studying and investigating the efficiency and economy of operations relating to all branches of the government.
- The Subcommittee is also tasked with studying and investigating the compliance or noncompliance with rules, regulations and laws.
- This includes oversight authority over cybersecurity in both the private and public sectors.

Equifax

- The breach itself exposed the financial and personally identifiable of over 145 million Americans. Sen. Carper's staff led the investigation, which focused on Equifax's failure to adequately emphasize cybersecurity company-wide.
- Equifax had **over 8,500** known medium, high, or critical vulnerabilities that it failed to remediate
- Equifax did not maintain a complete list of applications running on their networks.

FISMA Report

- Several months later, the Subcommittee conducted an investigation of executive agency compliance with the Federal Information Security Modernization Act or FISMA. The Subcommittee reviewed the past ten years of annual audits required by FISMA for DHS and seven other agencies.



Report Findings

- Of the eight agencies surveyed:
  - Seven agencies (STATE, DOT, HUD, USDA, HHS, ED, and SSA) failed to provide adequate protection of personally identifiable information.
  - Eight agencies (DHS, STATE, DOT, HUD, USDA, HHS, ED, and SSA) use legacy systems or applications that are no longer supported by the vendor making them vulnerable to a breach.
  - Five agencies (STATE, DOT, HUD, HHS, and SSA) did not have an accurate or comprehensive IT asset inventory of the applications running on its systems.
  - AND Six agencies (DHS, STATE, HUD, USDA, ED, and SSA) failed to timely install security patches that update the security of an application or program.

Links to PSI Cyber Reports

- PSI Website: https://www.hsgac.senate.gov/subcommittees/investigations/

- FISMA: https://www.hsgac.senate.gov/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf

- Equifax: https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf

Congressional Oversight as a Solution

Potential Promise and Problems

Kimberly Breedon & A. Christopher Bryant
Levin Center and Wayne Law Review
Congressional Oversight Webinar Panel on Cybersecurity
June 24, 2020

Public Confidence in Voting Systems

- Trustworthy and Trusted
- Effects of Cyberattacks or Threats of Cyberattacks on Public Confidence

Public Confidence in Voting Systems

- Recommended Best Practices for Election Security
- Current Practices and Vulnerabilities
- Election Officials' Potential Conflicts of Interest
- Proposed Legislative Fixes
- The Informing Function of Congressional Oversight as a Possible Remedy

Impediments to a Federal Statutory Fix

- THEORY: Tradition of state & local administration of elections
  - including federal elections
  - subsidiarity & participatory value to this structure
  - in any event, deeply embedded = resistant to federal intrusion

- Divided Government (& Congress) = enactment is politically impossible
  - clock is running out
  - but committee-driven oversight within control of either house

Hope for Oversight's Success

- What's the point?
- Need to spur state & local officials to action
  - draw public attention to neglect & conflicts of interest

- A job for Congress's
  - "Informing Function"

Woodrow Wilson on “Informing Function”

“**The informing function of Congress should be preferred even to its legislative function**. The argument is not only that discussed and interrogated administration is the only pure and efficient administration, but, more than that, that the only really self governing people is that people which discusses and interrogates its administration.”

The Informing Function's Dark Side

Senator Joe McCarthy (R-WI)

S Ct: Two Most Relevant Cases

- *McGrain v. Daugherty* (1927)
  - Teapot Dome Scandal; Senate investigation into now-resigned AG's passivity
  - Strong endorsement of implied congressional investigatory power
    - **In support of legislative function (including appropriations)**
    - Silent on informing public for informing sake
      - But public "embarrassment"/exposure no cause for halt of otherwise legit.

- *Watkins v. United States* (1957)
  - McCarthy Era case
  - Court reverses criminal conviction for contempt
  - **Gives mixed message on informing function**

Watkins (1957)

"That power is broad. It encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes. It includes surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them. It comprehends probes into departments of the Federal Government to expose corruption, inefficiency or waste."

Watkins, continued

"But, broad as is this power of inquiry, it is not unlimited. There is no general authority to expose the private affairs of individuals without justification in terms of the functions of the Congress. . . . Nor is the Congress a *law enforcement or trial agency*. These are functions of *the executive and judicial departments* of government. No inquiry is an end in itself; *it must be related to, and in furtherance of, a legitimate task of the Congress*."

Informing's Fine

But Exposing is Right Out!

???

What's A Conscientious Legislator to Do?

Informing

- Safe Harbors

Exposing

- Warning Signs

Safe (?) Harbors

- “governmental” v. “private” failures or malfeasance

- **a theoretical federal statutory response**
  - even if not politically practical or
  - structurally desirable

Warning (?) Signs

- Chilling exercise of constitutional rights?
- **Exposure to "punish"**

Comments?

Questions?

Answering the Clarion Call to Action: Congress's Role in Protecting Election Security

Prof. M. Tia Johnson
Georgetown Univ. Law Center

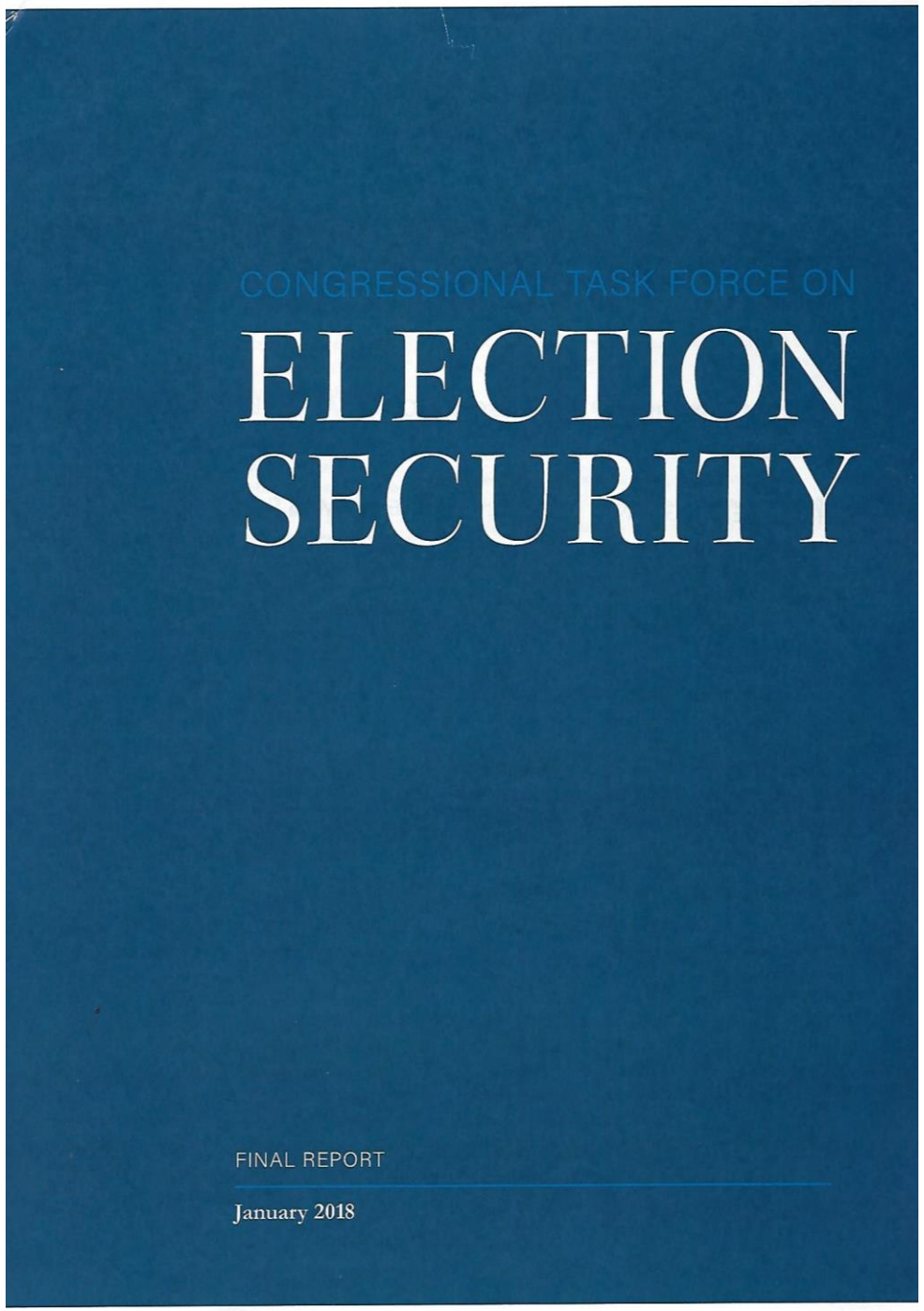
“On November 9, 2016, a sleepless night was ahead of us. And when around 8am the most important result of our work arrived, we uncorked a tiny bottle of champagne …took one gulp and looked into each other’s eyes… We uttered in unison: ’We made America great!’”

https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

Conclusions

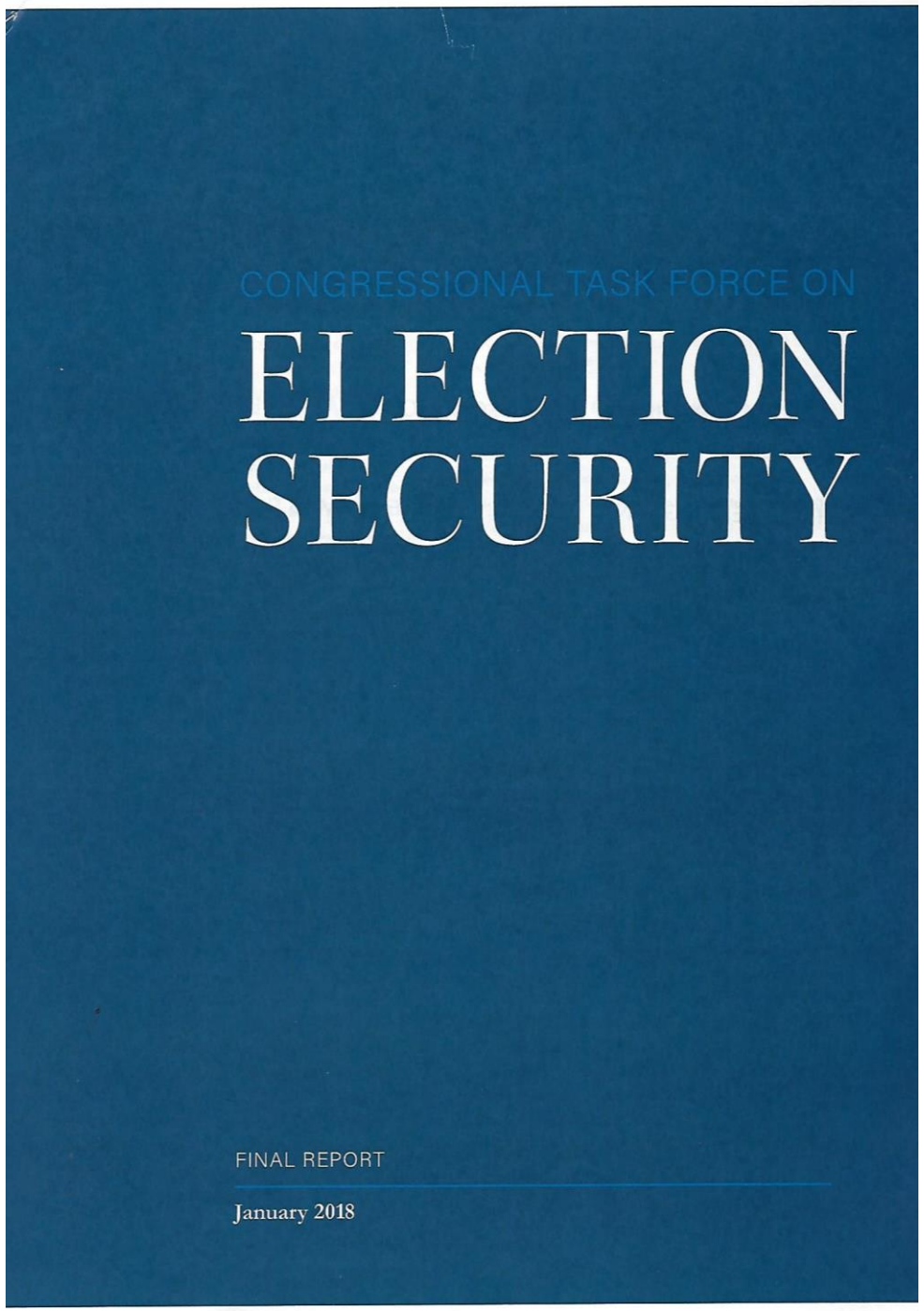
- Part I – Based upon the text and caselaw, Congress has broad authority to regulate federal elections and that federalism concerns are misplaced.

- Part II – discussed the multiple threats to the integrity of our electoral systems, threats that undermine its legitimacy, pose a national security , and call for immediate action to remedy.



Congressional Task Force on Election Security

"When a sovereign nation attempts to meddle in our elections, it is an attack on our country. We cannot leave states to defend against the sophisticated cyber tactics of state actors like Russia on their own."



Ten Recommendations

1. Federal funds should be provided to help states replace aging, vulnerable voting machines with paper ballots.
2. States should conduct risk-limiting post-election audits.
3. Federal funds should be provided to help states upgrade and maintain IT infrastructure, including voter registration databases.
4. Election technology vendors must secure their voting systems.
5. The federal govt should develop a national strategy to counter efforts to undermine democratic institutions.
6. The IC should conduct pre-election threat assessments well in advance of federal elections.
7. DHS should maintain the designation of election infrastructure as a Critical Infrastructure subsector.
8. Empower federal agencies to be effective partners in pushing out nationwide security reforms.
9. Establish clear and effective channels for sharing threat and intelligence information with election officials.
10. States should prioritize cybersecurity training.

TFES Recommendations

Recommendation		LATEST ACTION
#1	Federal Funds Should be Provided to Help States Replace Aging, Vulnerable Voting Machines with Paper Ballots	Consolidated Appropriations Act, 2020 (P.L. 116- 93, 12/20/2019)
#2	States Should Conduct Risk-Limiting Post-Election Audits	Consolidated Appropriations Act, 2020 (P.L. 116- 93, 12/20/2019)
#3	Federal Funds Should be Provided to Help States Upgrade and Maintain IT Infrastructure, Including Voter Registration Databases	
#4	Election Technology Vendors Must Secure Their Voting Systems	
#5	The Federal Government Should Develop a National Strategy to Counter Efforts to Undermine Democratic Institutions	National Defense Authorization Act for Fiscal Year 2020 P.L. 116- 92, 12/20/2019

TFES Recommendations

Recommendation		LATEST ACTION
#6	The Intelligence Community Should Conduct Pre-Election Threat Assessments Well in Advance of Federal Elections	National Defense Authorization Act for Fiscal Year 2020 P.L. 116- 92, 12/20/2019
#7	DHS Should Maintain the Designation of Election Infrastructure as a Critical Infrastructure Subsector	
#8	Empower Federal Agencies to be Effective Partners in Pushing out Nationwide Security Reforms	
#9	Establish Clear and Effective Channels for Sharing Threat and Intelligence Information with Election Officials	
#10	States Should Prioritize Cybersecurity Training	

WHAT REMAINS TO BE DONE

Bill Number	Name
S.2238/H.R.2722	Securing America's Federal Elections Act, legislation to help safeguard elections from foreign interference, which passed the House with bipartisan support.
S.2242	Foreign Influence Reporting in Elections Act, bipartisan legislation to require presidential candidates to report contact from foreign state actors to the FBI.
S.1247	Duty to Report Act, legislation to require candidates to report offers of assistance from foreign state actors to the FBI and FEC.
S.1540	Election Security Act, legislation to require paper ballots and provide election security grants
S.2669	SHIELD Act, legislation to prevent foreign interference in elections.

WHAT REMAINS TO BE DONE

Bill Number	Name
S.1060	DETER Act, legislation to combat foreign interference in our elections.
S.1356	Honest Ads Act, bipartisan legislation to apply the existing rules on disclosures in political ads on TV to those on social media platforms.
S.949	For the People Act, a sweeping package of pro-democracy reforms that aims to make it easier, not harder, to vote; end the dominance of big money in politics; and ensure that public officials work for the public interest.
S.890	Senate Cybersecurity Protection Act, bipartisan legislation to provide cybersecurity assistance to the Senate.
S.1834	Deceptive Practices and Voter Intimidation Protection Act, legislation to stop practices designed to prevent Americans from voting.

The Washington Post

"Russia is interfering in our elections again. And Trump supporters are emulating Russian tactics."

EVELYN FARKAS
MAY 17, 2020

https://www.washingtonpost.com/opinions/2020/05/17/russia-is-interfering-our-elections-again-trump-supporters-are-emulating-russian-tactics/?ceid=8335065&emci=d18000b1-3699-ea11-86e9-00155d03b5dd&emdi=5b156d04-5c99-ea11-86e9-00155d03b5dd

FOX NEWS
7:33 CT

Challenges for Oversight of Cybersecurity "Information Sharing"

Jonathan Lewallen
Assistant Professor of Political Science
University of Tampa

"Information sharing" as a policy alternative: development and difficulties

Applying congressional oversight tools to cybersecurity information sharing

- Hearings
- Investigations
- Nominations
- "Deck Stacking"
- Casework
- Budgets/spending

Why not centralize?

Information Sharing as a Cybersecurity Policy Alternative

"Information sharing" as policy alternative for cybersecurity

- multiple executive orders, Cybersecurity Act of 2015 Title I
- information being shared pertains to threats, vulnerabilities, defensive measures
- Vulnerability Equities Process, Automated Indicator Sharing programs, ISACs, privately-owned platforms

Reliance on information sharing is product of four dynamics:

- tradition of Internet self-governance and prevailing emphasis on minimalist legal environment
- Congress's inability to pass broader, more comprehensive laws (as in 2012)
- bounded rationality by policymakers: relationship to homeland security and "reasoning by analogy"
- authority given to defense, intelligence, homeland security, law enforcement agencies

Barriers to better information sharing:

- businesses may not see value of participation
- nature of some threats: information may be classified
- nature of the policy problem: information may not be shared until after threat has been remedied

General Challenges to Effective Oversight of Information Sharing

Lack of clear credit-claiming and position-taking opportunities for legislators

- members of Congress often derided for "only caring about re-election," but those incentives are important for constituent accountability and policy entrepreneurship
- in today's Congress, lack of a clear partisan dimension on cybersecurity information sharing may actually prevent oversight from taking place

How to measure successful oversight outcomes?

- "sharing more information" may be counterproductive
  - type/relevance of information more important than volume
- nature of the policy problem changes over time; the information that needs to be shared and success metrics may also change

How does Congress know if information is not being shared?

- legislature doesn't know what information *could be* shared but isn't, and neither do other groups by definition
- overlapping agency authority can create confusion about to whom Congress should turn
  - DHS has shared information about vulnerabilities in health care sector; Dept. of Defense working with banking sector

Challenges for Specific Oversight Tools

Hearings:
- limits on committee attention, need to hold hearings on other matters leads to lack of sustained oversight

Investigations:
- effective investigations can take months, years; nature of threats/vulnerabilities/information sharing can change during that time

Nominations:
- competition to define nominee priorities; no role for House committees

"Deck stacking":
- changing threats means uncertainty about which interests need to be included/favored in the future

Casework:
- limited constituent service opportunities; still voluntary for businesses

Budgets/"power of the purse":
- Congress can provide more funding, but reducing "wasteful" spending might hurt policy goals

Why Not Centralize?

Cybersecurity Solarium Commission report recommendation 1.2: create House Permanent Select and Senate Select Cybersecurity Committees

- meant to mirror Intelligence committees; committees would have legislative jurisdiction

In theory a centralized committee would address some concerns raised here

- would allow for sustained attention

Some practical issues with Commission's proposal:

- report says this proposal is not meant to take away from Armed Services or Intelligence Committees jurisdictions, so some overlap would remain
  - duplication/redundancy have value too; if one committee misses something, another committee might catch it
- chairs/ranking members of other cybersecurity-relevant committees would be *ex officio* members, which creates or maintains time and attention pressures; how involved would they be?
- adverse effects on other committees, issues, and capacity
  - if House Homeland Security Committee oversees parts of DHS but not CISA, what kind of members would want to serve on that committee? What would their goals be and how much would they participate?
  - Potential for confusion or strategic evasion by agencies: which committee would DHS respond to?

Thanks for joining us!

Levin Center at Wayne Law, https://law.wayne.edu/levin-center

Wayne Law Review, https://waynelawreview.org/