RTI INTERNATIONAL

April 2017

Understanding Demand for Cyber Policy Resources

RTI Report for the Hewlett Foundation's Cyber Initiative

Table of Contents

Tables

Executive Summary

RTI Report for the Hewlett Foundation's Cyber Initiative

Executive Summary

Cybersecurity is playing an increasingly critical role in our daily lives. Each year, more people in the U.S. and globally rely on cyberspace for personal and business activities, increasing the risks and costs associated with cyber in-security. And yet, many critical vulnerabilities in the internet infrastructure remain. In the U.S. today, by its own admission, the cyber policy community is not prepared to act efficiently and effectively to prevent, mitigate, and respond to attacks.

Cybersecurity decision makers inside and outside of government are frequently overwhelmed with information and opinions. As the overall quantity of information has been increasing, government officials are finding it more difficult to identify and interpret high value, usable information *(signals)* given all the useless information *(noise)* being promulgated. The current low signal-to-noise ratio in cyber policy makes it much less likely that high quality ideas, particularly from outside government, will reach government officials and impact policymaking.

Complicating the picture, few cyber researchers and policy experts outside of government understand either the specific needs and priorities of government officials, or the pathways to effectively communicate new information or ideas to them. As such, government officials' needs are not being fully met by the broader cyber policy community. In economic terms, the *supply* of cyber policy resources is not meeting the *demand* for such resources.

In partnership with the Hewlett Foundation, RTI International designed a study to assess the signal-to-noise ratio and identify the primary factors affecting supply and demand in the cybersecurity policy-making community. RTI conducted qualitative interviews with 39 current and former federal government officials in key cyber policymaking roles and 15 state government officials involved in cyber policymaking in California and Washington State. Interview candidates were identified through purposeful sampling and snowball recruitment, and as such, the results should not be viewed as representative of the entire government cyber policymaking community, in particular at the state level.

Interviews were conducted in late 2015 and early 2016, prior to President Trump and his Administration assuming oversight and management of U.S. cyber policy. As in past presidential transitions, this change could significantly affect the U.S. federal government's interpretation and implementation of policy. The results of this study should be interpreted in this context.

Study Goals

Federal and state government officials were asked a variety of questions related to how they engage with the cyber policy community inside and outside of government. The broad aim was to capture initial insights into the following questions:

Executive Summary

- How can non-government members of the cyber policy community make their work most useful to, and likely to be consumed and adopted by, government agencies?
- How do government officials communicate their needs and interests to those outside government? How could they improve?
- How do non-government cyber researchers and cyber policy experts communicate results and recommendations to government agencies? How could they be more effective?

Key findings from the federal government study and the case studies of California and Washington State are presented separately below. In the full report, they are described in separate volumes.

Federal Interviews: Key Findings

Interviews with key cyber policy officials in the federal government suggest that officials value much of the information and resources currently being produced by the cyber policy community outside government, but they expressed concern about academic research in particular—noting that it is often too theoretical, is not released quickly enough to be useful, and is not communicated in a way that highlights its value to policymakers. Conversely, industry was consistently praised for providing tailored data and recommendations, but criticized for being too biased. Policymakers voiced a strong desire for more research and recommendations that are applied, objective, and actionable.

Officials requested more research that focuses on either specific policy options being discussed inside government, or policy options that are more grounded in the current or near-term political environment. Others asked for more work that aims to connect basic, conceptual, and theoretical research to practical applications, through additional analysis and clearer communication.

Many of the findings of these interviews may be instructive to members of civil society working on U.S. cyber policy (researchers, policy experts, and advocacy groups), funders, and to the federal government. The following are some of key findings:

- Government officials view industry as having significant importance in cyber policy discussions for several reasons: industry controls the bulk of the cyber critical infrastructure, would bear many (likely most) of the costs of new regulations, collects more data in aggregate on cyber threats, and employs many of the most talented cybersecurity professionals.
- Despite the relative importance of industry, government officials trust information that comes from academics and think tanks more than that which comes from industry and advocacy groups. Officials believe that industry is particularly biased, only offering data and policy recommendations that will clearly benefit them and their bottom line.
- Industry experts are the most attuned to government needs and priorities: they frequently engage cyber policymakers, become well-informed about government's needs, and present relevant, valuable, timely, and actionable information and ideas. Comparatively, the structure of the academic environment (*e.g.*, publications are the primary metric of success) and academics' general lack of timely, relevant data make academics less agile in responding to specific government priorities.
- Legal restrictions on information sharing (requiring clearances) and a lack of understanding of technical cyber issues by members of Congress and their staff are recognized as significant barriers that restrict government officials from more fully engaging with and utilizing cyber expertise outside of government.

Federal Interviews: Recommendations

Based on our findings, the following specific recommendations are offered to members of civil society, funders, and the federal government:

- Government agencies should aim to more clearly specify and more widely advertise their needs among academic and think tank audiences, while academics and think tanks should focus more attention on interpreting "demand signals" from officials' statements and speeches.
- Given industry's perceived bias, academics (and think tanks to a lesser extent) have an opportunity to wield greater influence on government policymakers, if they focus their work more on policymakers' needs.
- Cyber experts outside government who seek to influence federal cyber policymaking should (a) identify the government cyber policy stakeholders in their particular area, (b) engage these individuals (or their designees) in meetings and listen to their priorities and needs, and (c) provide relevant information or feedback when possible.
- Academics and think tanks should aim to present their research and ideas in targeted,

Executive Summary

one-on-one briefings with policymakers, which officials considered the most effective form of communication. Brief one-page summaries of research findings were also considered particularly helpful.

- Industry and think tanks could help bridge the gap between academics and government. Think tanks should try to play more of an intermediary role, reaching out to industry for data, funding, and collaborative opportunities for their own use and for academics; meanwhile, academics should reach out more directly to industry on the same topics.
- More funding of cyber policy research is needed. Government itself is not funding enough cyber policy research, and other funders are not supporting enough policy research that specifically addresses government needs.

State Interviews: Key Findings & Recommendations

Cyber policymaking at the state-level is very different from the federal level for many reasons. Interviews with cyber policymakers in California and Washington State suggest that state governments' cyber policy structures and processes are immature as compared to those of the federal government. Critically, government officials and other state-level stakeholders need more support and resources that are aimed specifically at helping them develop and manage cyber policy at the state level, not at the national level. Broad differences in culture, priorities, and interests within state governments and the federal government create a considerable disconnect between cyber policymaking at each level, significantly limiting the use of shared resources. Further, states are very heterogeneous themselves—as state cyber policy initiatives mature, some states will provide new examples and resources to other states, but a wide variety of resources and support are needed given the differences that exist in state policy environments. The primary overlap needed at both the state and federal levels is more technical education for policymakers in federal and state legislatures, most of whom lack understanding of critical cyber technical issues.

Demand for Cyber Policy Resources: U.S. Federal Government

Volume 1

1. Introduction

1. Introduction

The fields of cybersecurity and cyber policy[1] are experiencing more activity than ever before. Companies, individuals, and governments are all discussing critical cyber threats and looking for solutions, and more researchers and other members of civil society are now focusing on cyber topics. Computer scientists, legal experts, political scientists, and economists are all studying cyber policy[1], and yet, the field remains immature. The reasons abound. The diversity of individuals and organizations involved in this field makes communication and coordination very challenging. Decision makers inside and outside of government are frequently overwhelmed with information and opinions, and they find good ideas difficult to identify, interpret, and use. While researchers are unclear about the specific needs of decision makers and pathways to communicate research findings to that audience.

This problem is not unique to cyber; funders and researchers have written extensively on the problem of "bridging the gap" between academia, think tanks, other nongovernmental policy organizations, and government stakeholders.[2] Although the issue is generic, cyber presents novel challenges. The technical and intangible nature of the internet makes establishing a baseline understanding of cyber threats, trends, and potential mitigation strategies more difficult. Too often, policymakers speak different languages—e.g., because terminology has yet to be standardized across the field or legal terms are being used indiscriminately or incorrectly by those in other fields, confusing the conversation. Further, the number of stakeholders and the breadth of competing interests and priorities are vast, and perhaps most critically, the roles of government, the private sector, and other actors are unclear and continue to be debated. In such a fluid space, new data, tools, structures, and processes are needed to better connect government and nongovernment members of the cyber policy community.

In partnership with the Hewlett Foundation, RTI International designed a study aimed at analyzing and characterizing the signal-to-noise ratio in the cybersecurity policymaking community. Government cyber officials today are often overwhelmed by the large quantity of information on cyber policy topics (e.g., new products, services, policy solutions, and opinions); however, the quality and usefulness of this information are often significantly lacking. This study explored ways to improve how information flows between government decision makers (on the demand side) and the communities working to support effective and efficient cybersecurity policymaking (on the supply side) to make the market for cyber policy information and resources more efficient and effective for all stakeholders.

RTI conducted a demand assessment of current and recent government policymakers across the federal government and two state governments, focusing on capturing initial insights into the following questions:

- How can non-government members of the cyber policy community make their work most useful to, and likely to be consumed and adopted by, government agencies?
- How do government officials communicate their needs and interests to those outside government? How could they improve?
- How do non-government cyber researchers and cyber policy experts communicate results and recommendations to government agencies? How could they be more effective?

[1] Note: In this report, we use the Hewlett Foundation's definition of cyber policy to include "topics that impact the security, stability, and resilience of a free and open Internet and connected devices." As discussed in the Foundation's 2016 revised strategy, this definition includes "traditional notions of computer and information security, but also the full range of related policy issues, such as Internet governance, net neutrality, encryption, surveillance, and privacy."

[2] See e.g., a 2008 paper by Joe Nye at http://www.jstor.org/stable/20447146 and a 2015 article by James Goldgeier and Bruce Jentleson at https://warontherocks.com/2015/06/how-to-bridge-the-gap-between-policy-and-scholarship/.

1. Introduction

In this volume, we present findings on the current stated needs[3] and broad priorities of U.S. federal cyber policymakers, their perceptions of the the nongovernmental policy community, and the channels of communication they use most. Based on our interviews, we also offer recommendations for several key stakeholder groups. Information from this report is intended to guide the thinking and resources invested in cyber by funders such as the Hewlett Foundation and stakeholders from the nongovernmental policy community, including academia, think tanks, and civil society organizations. We also identify barriers and enablers to decision making, some of which may be structural and require concerted effort from within and outside government to overcome. Where possible, we delineate between immediately actionable solutions and longer-term guidance.

In general, we find that current communication channels between the nongovernmental policy community and government agencies are poorly constructed or often nonexistent. Few government cyber officials clearly communicate the policy issues they are working on or what data, tools, or resources could most help them with policy decision making, and in many cases they may not know exactly what they need. Government cyber officials who do provide information on their priorities and needs often do so by releasing high-level strategy documents that rarely provide sufficient detail for the growing cyber policy community outside of government to develop highly responsive ideas and solutions. As such, these government officials often rely on trusted relationships and literature and internet searches when developing initial policy proposals, and they use public events and requests for comment once the proposals are well formulated or finalized. Poor demand signals create high barriers to entry for newcomers to the field, and in many cases, newcomers do not feel welcome by the cyber policy community.

However, existing cyber policy work by academics, think tanks, and civil society organizations often struggles to recognize the nature and characteristics of the policy environment and the need to propose solutions that are sufficiently actionable, constructive, and novel. Officials emphasize that funding ability and agency mandate serve as the key constraints affecting the adoption of new ideas. Both government and the outside policy community must learn to recognize and work within these parameters

Hewlett Cyber Initiative

The Hewlett Foundation established the Cyber Initiative in 2014 to increase the production of ideas in cyber policy. Since March 2014, the Foundation has issued grants to academic, advocacy, think tank, and civil society organizations, with the goal of cultivating a field to develop thoughtful, multidisciplinary solutions to complex cyber challenges and catalyze better policy outcomes.

1.1 Study Methods

RTI conducted semistructured interviews with 39 individuals in the federal government and 9 informational interviews with individuals outside of government. At the time of the interviews, government officials interviewed were serving in their positions; however, we also interviewed several officials who had recently exited government to gain additional perspectives. Before the government interviews, RTI conducted several informational interviews with stakeholders in academia, civil society organizations, and the private sector to understand current outreach activities and challenges faced from the "supply side" of information flow. Table 1-1 provides a summary of interviews conducted by broad category. Participants were guaranteed anonymity, so neither the name nor the organizational affiliation of participants is listed in the report.

After consulting with subject matter experts, RTI initially identified key agencies within the cyber policy community and then leveraged contacts across existing networks to identify the appropriate positions and individuals within each agency. In many cases, we used a snowball technique to identify second-degree connections for interviews. Out of 44

[3] Importantly, this study focused on developing a better understanding the characteristics of government officials' demand (or stated need) for cyber policy information and resources, based on interviews with a set of key officials. No attempt was made to objectively assess what government officials need independent from what they say they need.

1. Introduction

requests, we received one nonresponse and four refusals. Efforts were made to maintain a representative distribution of relevant cyber agencies within the interviewee sample and seek out top-level decision makers within each agency. Interviewees were informed of and asked to acknowledge confidentiality and anonymity protocols and had the right to refuse to answer any question or end the interview at any time. Other than themes summarized in this document, interview content was not shared outside of RTI's internal team and Hewlett Foundation staff.

Table 1-1 Federal Case Studies: Interview Sample Characteristics

CORE INTERVIEWS	**39**
Current government officials	33
Former government officials	6
INFORMATIONAL INTERVIEWS	**9**
Academia	2
Think tanks and foundations	6
Media	1

Interview guides were developed after a series of formative interviews; literature review of evaluation research; and a consultative workshop with Bay Area cybersecurity professionals, researchers, and former government staff and officials.

Interviews themselves were approximately 1-hour long and were conducted by site visit or phone call, according to interviewee availability and preference. In most cases, an RTI interviewer was accompanied by a note taker. Transcripts from each interview were then cleaned and coded in NVivo qualitative coding software. RTI subsequently undertook theme-based analysis.

In the questions posed to participants, the term "cyber" was intentionally left up to individual interpretation. As a result, and in line with the Hewlett Foundation's definition of "cyber policy" (described above in footnote 1), "cyber" enjoys a broad interpretation for the purposes of this report. We aggregated and summarized the qualitative findings from the study below. Responses are presented thematically so that recurring themes in the analysis are highlighted. Although we make a few illustrative points, no responses should be interpreted as being representative of federal or state governments, of any agency within the government, or of any particular industry that falls under the broad interpretation of "cyber."

In addition to the interviews conducted for this study, we conducted secondary research for background purposes, focusing on recent cyber policy documents and information produced by the cyber policy community; additional research helped supplement and better characterize information collected during the interviews.

1.2 Study Limitations

The results of this study are based on qualitative research conducted using a combination of purposeful sampling, convenience sampling, and snowball recruitment. All of the interviews were conducted using a semistructured interview guide; the questions asked were primarily open ended, and the interviews differed in focus based on the participants' knowledge, experience, and willingness to provide specific answers. In some cases, individuals were unwilling to answer certain questions. Some of the interviews were conducted by phone and others were conducted in person.

The methods used were appropriate given the exploratory nature of this study; however, given the lack of a robust sampling strategy (e.g., based on quantifiable selection criteria) and given that the exact questions asked to each participant differed, our findings should be interpreted as necessarily subjective, providing an initial view into the government cyber policy-making community.

1.3 Study Scope

The cyber field faces a broad challenge of establishing strong channels of information flow for optimal decision making. Information flow itself is not unidirectional and change may come from diverse sets of actors. In this study, however, we focused primarily on how information produced by the nongovernmental policy community (focused primarily on academia, think tanks, and other civil society organizations) can be designed and communicated more effectively to potential government consumers. Stated in economic terms, we assumed that the government's demand for information and tools to support cyber policymaking is not being met by the supply of such resources by the nongovernment cyber policy community (see more discussion in text box on page 12).

Cyber Policy Supply and Demand: Does a Market Failure Exist?

Using economic concepts of supply and demand to describe the market for cyber policy resources provides a helpful framework through which to analyze many dynamics at play; however, it is important to recognize that the market for cyber policy resources is much more complicated than a casual use of these terms may suggest.

Assuming that a market failure exists, it could be explained by a wide variety of factors. Based on our interviews, one critical factor is the lack of sufficient funding to support cyber policy research and analyses of interest to government officials (demand). The government is not funding enough cyber policy research directly, and other sources are not funding cyber policy research based explicitly on government demand. As such, existing and ongoing cyber policy research is principally focused on areas of interest to funders and to the researchers themselves, when the funders are less prescriptive in their funding solicitations.

The nongovernment cyber policy community still does have an interest in producing information and tools that the government finds valuable—for example, in order to receive accolades, to see their work have an impact, and to generate more funding, directly or indirectly. However, information asymmetries may be preventing a better functioning market in this case. Information asymmetry is a type of market failure that occurs when a buyer or user (demand) has important information that the seller (supply) in a market does not or vice versa. In this case, information asymmetries may exist in both directions.

Individuals in the nongovernment cyber policy community (supply) do not know what the government (demand) wants. Government officials do not provide enough information on their interests and needs, often because of a lack of time or legal restrictions; thus, individuals outside of government who are aiming to provide useful information to government often do not hit the mark. In this case, the cyber policy community often focuses on issues that are of broad interest to the public, as described by the media, as a gauge for government demand.

In the other direction, many government officials (demand) do not know how best to identify cyber policy research and tools that would be most useful to them. The amount of research and number of tools developed are large, and officials lack the time and mechanisms to review all of the information being produced; therefore, government officials often use various signals to identify potentially valuable cyber policy research. In this case, signals—which provide buyers or users with an indication of the quality or value of a product or service—include suppliers' personal reputation and the brand or reputation of their organization. Government officials often repeatedly engage individuals who are well known and respected and the organizations with a highly reputable brand. Consequently, suppliers without such brands may find it very challenging to solicit the attention of government officials effectively.

The majority of the recommendations presented in this report focus on adjustments that could be made to the supply side: the broader policy community generating ideas. However, we recognize that various theories-of-change frameworks call for exogenous shifts in the policy environment or adjustments on the government or "demand" side, so we do focus some attention on this side of the market for cyber policy resources.

Little past evaluation work assesses this information disconnect in cyber. In other sectors such as public health, researchers have used a prevention model to implement strategies and promote health behaviors. Scholars at the Centers for Disease Control and Prevention use surveillance, risk factor identification, intervention, and evaluation activities. These technical (medical) and nontechnical research, analysis, and evaluation projects are interwoven to foster more effective interventions when placed in the community. We pull from these previous efforts to structure recommendations based on existing enablers and barriers to idea adoption in the cyber field.

2. The Cyber Policy Community Outside Government

2. Cyber Policy Community Outside Government

Actors outside government play important roles in influencing and reacting to cyber policy, particularly as a result of the field's newness and its multistakeholder, decentralized nature. Government attention is both demanded by and drawn to different interest groups. In Table 1-2, we characterize many of the key players in cyber today, and Table 1-3 provides a summary of the types of outreach activities in which these groups engage.

Each of these groups has its own role and contributions related to cyber policy. Many interview participants stated that organizations and individuals outside of government—both private-sector organizations and other nongovernment organizations working on cyber policy—are having a greater impact on cyber policy. One government participant went so far as to say that "government policymakers are no longer the critical players in this space anymore. If you actually want, if you care, to make a difference, you don't do it through government." Most government officials and other individuals interviewed for this study had a less polarized view of the role and influence of government, and two individuals noted that the private sector highly values

Table 1-2 Overview of Key Stakeholder Groups Outside of Government

STAKEHOLDER GROUP	DESCRIPTION
Private sector	
Cybersecurity companies	Companies that sell cybersecurity products or services (e.g., FireEye [including Mandiant], Intel Security [formerly McAfee], Symantec, Tanium).
Consultancies	Companies that provide consulting services on cybersecurity strategy and implementation activities (e.g., PwC, Deloitte).
Other companies with cyber offerings	Companies that are not primarily focused on cybersecurity but are heavily involved in providing cybersecurity products and services to their customers, such as internet service providers (ISPs) (e.g., Verizon) and operating system developers (e.g., Apple, Google, and Microsoft).
All other private companies	All private companies can be affected by cybersecurity attacks, but those that are of most interest to the government/policy community are part of the U.S. critical infrastructure (e.g., finance, utilities) or are technology companies.
Independent security researchers ("hackers")	Security researchers play many important roles in the cyber policy community, such as helping identify new potential threats and solutions. Within this group, so called "white hat hackers" look for vulnerabilities in private and public networks (often paid through bug bounty programs).
Academic institutions	Academic centers usually focus on activities, such as conferences and workshops, that facilitate conversations about cybersecurity and support collaboration.
Academic researchers	Individual researchers at academic institutions (usually funded through grants) produce data, analyses, and expert opinions.
Think tanks & research/policy firms	Think tanks (usually nonprofit) conduct policy-relevant research and analyses on issues like national and homeland security, counterterrorism, and cybersecurity issues.
Advocacy groups	Advocacy groups are either private or nonprofit organizations that usually focus on a small number of core issues, which they advocate for, and governments are their primary targets.
Media	Media organizations provide a critical channel through which government officials learn about new products/services, research, and public/industry perspectives, and nongovernment stakeholders learn about government action and interests. Media stories can play a large role in policy debates.

2. Cyber Policy Community Outside Government

experience working on cyber policy in the government, motivating some thought leaders in academia and the private sector to seek a stint in government to bolster their credentials. Such examples suggest that despite the large role of the private sector in cyber policy, government cyber policymakers are perceived as playing an important role.

Table 1-3 Summary of Output and Outreach Activities of Nongovernment Organizations

OUTREACH OR OUTPUT	PRIMARY ACTORS
Publications and written work (public)	Academic and research institutions, private industry, think tanks
Networking events (public)	Think tanks, industry and professional/trade associations
Networking events (private)	Industry and professional/trade associations
Education and training	Academic institutions, think tanks
Lobbying	Private industry, advocacy groups, industry and professional/trade associations
Data collection, provision, and analysis	Academic institutions, private industry, think tanks, trade associations
Briefings	Private industry, academic institutions, think tanks

Role of Private-Sector and Third-Party Firms

Private-sector companies play a critical role in any cyber policy discussion. Organizations in the private sector control the bulk of the critical infrastructure in the United States, and our interviews suggest that government officials widely believe that private companies hire many of the best cybersecurity analysts, have the best (i.e., most relevant) data, and come up with the deepest insights when cyber events occur. Many private-sector organizations frequently meet with government officials to discuss cyber policy issues. The private sector as a group is often considered to be fearful of unnecessary regulation, wary of public discovery should proprietary information be stolen in a breach, or (post-Snowden) skeptical of cooperating with policies that may be perceived to infringe on individual digital rights. Meanwhile, the products that private companies create and sell to consumers may contribute to cyber insecurity: the products they sell might disrupt or challenge the current cyber policy status quo or lack adherence to voluntary standards or best practices, without significant consideration of their consequences from a social perspective.

A variety of factors seem to be affecting the outsized role that industry plays; the following are some examples of what we heard:

- **Industry often hires former government officials.**
- **Industry reaches out to government often (i.e., so they know what government is thinking/working on).**
- **Industry tailors comments to what government is working on/asking for (very applied/relevant).**
- **Industry sometimes offers new data that government does not have.**
- **Industry provides technical input/feedback.**
- **Industry provides input/feedback on the potential impact for their business/the economy.**

3.
The Cyber Policy Community Inside Government

3. The Cyber Policy Community Inside Government

The process by which the U.S. government makes new cyber policies is complex and is not homogenous across the government. Very structured processes are used to manage the design, development, refinement, and approval or rejection of potential new policies (such as new laws or regulations); however, informal processes play a big role as well, particularly when a new policy is first discussed within a certain agency. Our interviews with senior government officials working on cyber policy helped us map out much of this process and identify characteristics that are important for the community outside of government to understand to better consider how to engage with and influence government policymaking.

The goal of this section of the report is to provide a broad overview of and key insights into the process by which the U.S. government designs and develops cyber policy. We hope this discussion can serve as a primer to individuals and organizations outside of government as they seek to understand how their work could be refocused to be more useful to the government and how to communicate new ideas, tools, or other research or analysis findings to the government.

How are specific agencies involved in cyber policymaking?

A variety of factors determine the role that a particular person or agency plays in cyber policymaking and ways that person or agency engages with individuals and organizations inside and outside of the government. Some of these factors are based on the person's or agency's work style and personality, and other factors are based on more easily discernable characteristics such as whether the agency is a regulatory agency.

The following key government agencies are active in cyber policymaking:

- **National Security Council (NSC)** provides leadership from the White House by coordinating government and industry stakeholders and designing new cyber initiatives and policies for agencies to implement.
- **National Institute of Standards and Technology (NIST)** develops Federal Information Security Management Act (FISMA) standards that apply to federal civilian IT systems and standards and frameworks that are often widely adopted by industry.
- **Office of Management and Budget (OMB)** is responsible for overseeing implementation of FISMA standards by federal civilian IT systems.
- **Department of Defense (DoD)** is responsible for military cyber defense and for the security of national security systems, which handle classified information.
- **Department of Homeland Security (DHS)** has operational responsibility for protecting federal civilian IT systems and is the lead agency coordinating federal efforts to help the private sector protect critical infrastructure assets under private sector control.
- **Department of Justice (DOJ)/Federal Bureau of Investigation (FBI)** are the leads for enforcing relevant laws.

Hierarchically, the White House has played a coordinating role in developing cyber policy for the executive branch of government, and this role is managed by the NSC within the White House. The NSC primarily comprises detailees[3] who develop government policies and strategies that are used by the rest of the executive branch to set their priorities and, in some cases, are used by Congress to develop new laws and regulations. The NSC does not have a budget to contract research studies, so instead they leverage secondary research and trusted relationships—both within the government and outside the government—when developing cyber policy.[5] Reliance on a small number of trusted advisors was a theme we heard in our interviews from many different individuals throughout the federal government.

Most agencies play more specific roles, generally dictated by their Congressional mandate (key roles outlined in statutes and some specific activities requested in federal budgets) with additional direction coming from the White House. Table 1-4 provides a summary of all of the government departments, agencies, and subagencies that were targeted for this study because they were considered by the project team and the Hewlett Foundation to be particularly important to cyber policymaking.

A number of factors determine how and how much agencies engage with organizations and individuals outside of government before making cyber policy decisions. For example, is a security clearance required? How much

[4] Detailees officially work for other government departments such as the DoD and DOJ but are supporting the White House as a liaison, on loan from departments with a security role.

Cybersecurity Information Sharing Act (CISA) of 2015

As written into law on December 18, 2015, CISA was intended "to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats." The law has two main components, as follows:

1. Authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats.
2. Provides certain protections to encourage companies to voluntarily share information—specifically, information about "cyber threat indicators" and "defensive measures"—with the federal government, state and local governments, and other companies and private entities.

The law requires companies to remove any personally identifiable information from the data they share with the government to qualify for the protections. By guaranteeing protection from prosecution, the law is intended to encourage businesses to share more information on cybersecurity, thus broadening everyone's knowledge and ability to respond to possible threats.

What roles did key government and nongovernment organizations play?

Our interviews suggest that CISA was delayed and watered down because of feedback received from industry and industry groups. The idea of information-sharing legislation was discussed starting in 2009, but no information-sharing law was passed until CISA. Several officials stated that industry opposition and the federal government's (and in particular Congress's) lack of understanding of cyber resulted in a 6-year-long effort to pass legislation and a bill that would have very little impact. Highlighting the lackluster nature of the final bill (CISA), these officials noted that many of the issues the bill aimed to address had largely been addressed by other initiatives in the public and private sectors and the final bill was limited only to liability protections, as a result of industry opposition.

In January 2015, the idea of information sharing began to gain momentum. The White House released an "Information Sharing Legislative Proposal" and, then a month later, issued an Executive Order on information sharing. By June, the House and Senate had passed information-sharing bills, and by December, CISA was signed into law by the President.

In the midst of this process, the Center for Security and International Studies (CSIS) convened three workshops to discuss the technical, structural, and legal challenges to cyber threat information sharing; attendees included representatives from government, industry, and privacy organizations. In March 2015, CSIS released a report entitled "*Cyber Threat Information Sharing: Recommendations for Congress and the Administration,*"[1] which helped speed up the development and passage of cyber-policy related bills in Congress.

The U.S. Chamber of Commerce also played a key role in getting broad industry support for CISA, according to several officials, although two officials stated that the Chamber's involvement and lack of technical understanding made the process more confusing to many members of Congress. In the end, CISA was supported by the Chamber, as well as by the National Cable & Telecommunications Association and the Financial Services Roundtable. However, a number of companies opposed the bill, including Twitter, Yelp, and Apple, as did civil liberty groups such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation.

In two letters to Congress,[2] a large number of academics and security experts expressed their opposition to CISA, focusing on concerns about privacy and civil liberties infringement, and government officials noted that these letters did result in some changes in the legislation.

What are key takeaways from this example?

Policymaking can take a very long time, requiring lots of patience; industry plays a very large role in guiding policy debates, sometimes overshadowing most other perspectives; and academics and members of civil society can directly affect government policy.

[1] See more here: https://www.csis.org/analysis/cyber-threat-information-sharing.

[2] See the letters here: http://cyberlaw.stanford.edu/blog/2015/04/technologists-oppose-cisainformation-sharing-bills and here: https://www.elon.edu/e/CmsFile/GetFile?FileID=202.

NIST Cybersecurity Framework of 2013

The NIST Cybersecurity Framework, created through collaboration between government and the private sector, aimed to use a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. Since its release, it was been widely praised and adopted by industry. The Framework aimed to provide organizations—of any size, degree of cybersecurity risk, or cybersecurity sophistication—with risk management principles and best practices that could be used to improve the security and resilience of critical infrastructure and help organize and structure multiple approaches to cybersecurity by assembling the many standards, guidelines, and practices that were already working effectively in industry.

Many government officials interviewed mentioned the NIST Framework as an example of good public policy, noting that it was developed by government and leveraged significant input and feedback from industry and other members of the nongovernment policy community. However, several officials noted that the impact of the NIST Framework has not been significant and organizations that have adopted it already had most, if not all, the recommend structures and policies in place already.

What roles did key government and nongovernment organizations play?

In February 2013, the White House released an Executive Order that motivated the development of the NIST Cybersecurity Framework, and according to multiple officials, one major reason for the eventual success of the Framework was that the model used had come out of the think tank community and already had the support of many industry stakeholders. In 2008, CSIS released a recommendations report for the incoming administration entitled "Securing Cyberspace for the 44th Presidency."[1] This report was based on multiple CSIS-organized convenings, including with industry; thus, industry's perspective on the model proposed in the NIST Framework had been taken into account.

Between February and July 2013, when NIST released the first draft of the Framework, many organizations outside of government—including think tanks, industry, academia, and advocacy groups—had an impact on the development of the framework, which was managed by NIST, DHS, and the White House. According to multiple government officials, one of the biggest reasons for the success of the Framework was the extensive informal review process used to solicit feedback on early versions of the Framework, which were leaked to outside groups. This process allowed NIST to review, respond to, and make changes to the Framework based on feedback received from outside organizations, before the original first draft was released in July.

Beyond CSIS, several organizations were particularly helpful during the development of the Framework. The Center for Democracy and Technology and the ACLU both provided constructive input and feedback. From industry, Intel and Bank of America were very involved. From academia, several workshops were held at universities, but the only academic institution that played a significant role in crafting the Framework was Carnegie Mellon, which had developed a maturity model that was very useful in developing the Framework.

What are the key takeaways from this example?

Government policymaking efficiency (and possibly effectiveness) benefits significantly when input and feedback are solicited early in the process, before formal mechanisms are used; industry buy-in can enable rapid policy progress; and academics and members of civil society can have a direct and significant impact on government policy, even at early stages of development.

[1] See more here: https://www.csis.org/analysis/securing-cyberspace-44th-presidency.

3. The Cyber Policy Community Inside Government

time do policymakers have before they need to make a decision? Does the agency fund external research? Table 1-5 provides a summary of key factors that affect the frequency and types of engagement agencies have with external organizations, based on our interviews and supplemented by secondary research.

Examples of cyber policymaking in the U.S. government

The U.S. government sets policy on cyber issues in many different ways: through legislation, White House or agency policies or guidelines, mandatory and voluntary standard operating procedures, or selection of judicial or civil cases to pursue. Two policy examples discussed on the following pages help ground this discussion by explaining the process by which these policies were developed and the roles that different government and nongovernment organizations played: Cybersecurity Information Sharing Act of 2015 and the NIST Cybersecurity Framework of 2013. These examples are not intended to be representative of the processes by which cyber policy is made across the government; however, both offer many lessons on the policymaking process and the roles that individuals outside of government can play.

Career Bureaucrats versus Political Appointees

Within the government, several classifications for individuals are important to understand when engaging in discussions about policymaking. Some individuals involved in cyber policymaking are career bureaucrats, who have strong job protections and often have worked in the government for many years. These individuals are found throughout various government agencies and understand government policies and procedures very well. According to one political appointee, these individuals are more willing to take risks because they do not have much to lose (i.e., it is difficult to fire them), although other interviewees offered the opposite perspective (see below).

Political appointees are usually linked to the current administration and tend to serve shorter terms of service. Individuals working in the White House and in advisory or top leadership positions within agencies are usually political appointees, often with specifically termed appointments of 1 to 2 years (the average time is 18 months) or appointments that will end at the end of the current administration if not sooner. Individuals working as fellows in the government are similarly not in career-track positions; fellowships are usually termed positions. In direct contrast to the statement above, several interviewees noted that political appointees and fellows tend to be more willing to push the envelope because they are not trying to make a long-term career out of their current positions. One interviewee noted that fellows often join the government temporarily with a strong interest in advancing one or more specific policy aims.

> Several interviewees noted that within Congress, many (possibly most) of the Members of the House and Senate have no real understanding of cybersecurity threats or solutions.

Temporary positions such as political appointments and fellowships can offer a mechanism for sharing information between the government and nongovernment policy communities, as several interview participants noted. Academics entering the government as political appointees can provide a very helpful connection between the two communities, and if they return to academia once their appointment ends, they can continue to serve in this role or bring this perspective with them. However, other participants noted that involving political appointees (particularly short-duration fellowships) in cyber policymaking has drawbacks because agencies invest in them but then lose them after a short period of time, and knowledge transfer back to the agency does not happen often.

Additional disagreement exists regarding the value that temporary fellows and political appointees offer the policy process. Several interviewees stated that academics who move into government for a year-long (or sometimes only 9-month long) fellowship can cause problems because they do not fully understand how government works but may believe they do. However, others stated that academics who work for government agencies

[5] Of note, according to one interviewee, the NSC cyber group primarily comprises individuals with a legal or policy background, and currently this group does not include anyone with a computer science background.

3. The Cyber Policy Community Inside Government

Table 1-4 Overarching Categorization of Key U.S. Government Agencies Active in Cyber Policymaking

CLASSIFICATION GROUP	KEY AGENCIES	SUMMARY DESCRIPTION
Defense/intelligence	Department of Defense (OSD, CIO's office, AT&L, NSA, CIA, Cyber Command), ODNI	Deter and mitigate cyber events aimed at the U.S. through intelligence gathering and possibly offensive cyber intrusions. Play a core role (probably the most influential) in cyber policy development, for example, by requesting new capabilities/authority or describing the impact of certain policies on our defense and intelligence abilities. Maintain the security of their own networks.
Regulatory/enforcement	Treasury Department, FCC, FTC, SEC, OMB	Play a direct role in regulating individuals and/or organizations, which can restrict their ability to engage in private and/or informal discussions about cyber policy issues. Often public comments are requested through a very open process after draft policies are developed. In many cases, engagement with nongovernment groups is focused on industries being regulated, with minimal interaction with academic/think tank communities. (NOTE: OMB is the only agency in this group that is focused on enforcing standards adherence [e.g., FISMA] by government agencies.)
Technology policy/standards development (nonregulatory)	Department of Commerce (Office of Secretary, NIST, NTIA), OSTP	Provide support to industry and citizens through the development of new standards, support for new technologies, and development of new technology policies aimed at improving the efficiency or effectiveness of society (e.g., by reducing the cost of cybersecurity). Interact frequently with industry.
Law enforcement	DOJ, FBI, USSS	Law enforcement agencies (DOJ, FBI, USSS) investigate and prosecute cases of cybercrime. Cyber policy is primarily influenced through choice of litigation and gaps in the ability to gather intelligence and evidence and conduct successful prosecutions.
Homeland security	Department of Homeland Security (HSARPA, NPPD)	Support private companies and public organizations (e.g., state governments) by helping to develop, implement, and share technologies and policies that enable better proactive and reactive cybersecurity. Work closely with other sectors (e.g., financial, commercial, state governments) as owners of critical infrastructure.
Legislative branch	House and Senate member and committee offices	Primarily influence cyber policy through bills/potential legislation, including through the federal budget approval process. The choice of hearings to be held and individuals selected to speak at hearings provides legislators additional influence. Legislators offer one of the most direct ways for specific citizens' cyber-related concerns to be raised and considered.
White House	NSC	Plays a key role in coordinating the development of broad cyber policies to be implemented by one or more executive branch agencies and to be coordinated with the intelligence community across the government to provide input and feedback on cyber issues.
Other executive branch	State Department, NSF, NAS	Various other agencies play key roles in supporting the development and implementation of cyber policies. The State Department is working to integrate cyber into our diplomatic strategies and may plan a large role in future cyber policy initiatives. NSF and NAS oversee new research to improve cybersecurity for all U.S. stakeholders.

Note: Inclusion in this list does not confirm participation in the study, and exclusion should not suggest that agencies are not involved in cyber policymaking. Appendix A defines the agency abbreviations.

3. The Cyber Policy Community Inside Government

Table 1-5 **Characterizing U.S. Government Agencies Active in Cyber Policy: Factors that Affect External Engagement**

Barrier ● Incentive/Facilitator ● Combination ●

AGENCY	REGULATORY AGENCY?	SECURITY CLEARANCE REQUIRED FOR MOST DISCUSSIONS? (OR REGULATORY RESTRICTION ON SHARING)	SPEED IS CRITICAL—MOST CYBER ACTIVITIES ARE REACTIVE WITH NO TIME TO ENGAGE WITH EXTERNAL COMMUNITY?	FREQUENT FORMAL ENGAGEMENT WITH EXTERNAL COMMUNITY?	EXTERNAL ENGAGEMENT IS ALMOST EXCLUSIVELY WITH INDUSTRY?	FUND EXTERNAL RESEARCH TO SUPPORT CYBER POLICYMAKING?
Commerce				● ●	●	● ●
Congress				● ●		●^
DHS				● ●		● ●
DOD		● ●	● ●			●
DOJ						●
FCC	●			●	●	
FTC	●			●		
NIST				● ●		● ●
NSC		●				
NSF				● ●		● ●
NTIA				●		●
ODNI		● ●	●			
OSTP				●		●
SEC	●				● ●	
State Department			●	●		
Treasury	●	●*		●	● ●	

* The Treasury Department cannot discuss if/when cyber-related sanctions are considered.

^ Congress can authorize or request agencies conduct certain research but cannot directly fund external research.

3. The Cyber Policy Community Inside Government

often have more expertise and experience in a given area than the existing government staff, which can cause friction.

Technical Cyber Experts and Nontechnical Cyber Experts

The particular combination of educational background and experience of each individual has a significant influence on the frame of reference that each uses to consider and discuss cyber issues and potential cyber policies. The good news is that most of the individuals working in key government positions on cyber policy seem to have at least a moderate conceptual understanding of many critical technical issues, of policymaking, and of other important nontechnical issues (e.g., economic considerations). However, most of these individuals appear to lack needed depth of expertise in one or more of these perspectives. In many cases, these individuals have staff working for them or trusted advisors who help fill gaps in understanding; however, our interviews suggest that this is not always the case. Several interviewees noted that the biggest gap is technical; there are relatively few technical cyber experts in key positions; however, this imbalance appears to have improved recently.

As an example of this technical gap, several interviewees noted that within Congress, many (possibly most) of the Members of the House and Senate have no real understanding of cybersecurity threats or solutions.

To make up for this deficit, they rely heavily on staff members to provide technical guidance; however, interviewees noted that Congressional staffers with strong technical understanding of cyber issues rarely stay in government for long before moving to industry, likely motivated by much higher salaries, among other reasons. The void created by their hiatus is both immediate and longer term in that few individuals left in government roles understand the issues, and institutional knowledge is damaged.

Looking at Trends: How is Cyber Policymaking Changing?

In 2013, the Government Accounting Office (GAO) released a report entitled *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*.[6] Our interviews, conducted mainly between January and April 2016, suggest that the community of individuals working on cyber policy within the government believes that some of the deficiencies described by the GAO report in 2013 have improved over the subsequent 3 years. Officials interviewed broadly agreed that cyber policy has become a much higher priority inside government in recent years, that government roles and responsibilities are now better defined, and that communication both within government and with outside stakeholders has increased in quantity and quality. However, many individuals felt there is still significant room for improvement.

When considering how the environment for cyber policymaking has changed and will change in the future, two interview participants suggested that broader changes in government and perceptions thereof should also be considered. Both individuals noted that recent changes in opinion within and outside of government are shifting toward a smaller role for government in many policy debates, pushing elected officials and government employees to focus on solutions that do not involve government using a heavy hand (e.g., through new regulations).

Based on statements made by the Trump administration thus far, it seems likely that this administration will broadly look to deemphasize the role of government in addressing many policy issues; however, on security issues, the administration seems to support a strong role for government. This could include cyber policy as well.**How does government consume cyber policy information today?**

Government stakeholders consume information from a wide variety of sources for many different purposes. The type of information consumed could be information on a certain type of threat, affected group, or potential technical or policy solution. Participants consume information both **actively** (in response to an event or a specific White House or agency initiative) when the focus is on potential solutions to a particular problem/concern and **passively** (without regard to any specific need/use) such as information on threats, affected stakeholder groups, and solutions.

Actively Seeking Information

When an event happens or when a particular threat or type of solution is prioritized, key individuals in government who are looking for input and feedback tend to consult people they trust inside government, outside government, or both. The majority of interview participants indicated that they reach out to trusted contacts as their first source of information or one of their first sources. At these times, speed and the need for secrecy can cause government stakeholders to spend little time reaching out to a broad group of individuals outside of government in particular, unless they are required to do so.

3. The Cyber Policy Community Inside Government

Passively Consuming Information

In contrast, many government stakeholders consume swaths of information passively. Most of the interview participants indicated that they routinely take in information passively by learning from other government stakeholders, for example, during briefings at interagency meetings, and by reading information trusted sources send them. Trusted sources might send information/results that they authored, or they might forward information to government stakeholders that they found useful.

In Table 1-6, we list policymakers' main mechanisms for consuming cyber policy information and information resources. Throughout our interviews, people noted that communication was difficult for several reasons:

- Formal structures do not exist to communicate with agencies.
- Structures that did exist were not used by all relevant outside organizations.
- Permitted channels of communication were limited by federal law.

Despite these barriers, policymakers frequently access a combination of written and verbal communication via the platforms listed in Table 1-6.

Modes of Communication Used

Our interviews highlighted and characterized a wide variety of communication mechanisms that government policymakers use to consume cyber policy information. The following sections summarize the most frequently mentioned mechanisms.

Informal routine intake. Most agencies have existing email digests and listservs circulating, which provide them access to recent relevant research and analysis. Other informal channels include Twitter feeds, blogs, and external digests that present curated information. Officials noted certain blogs were valuable for presenting novel and insightful perspectives. They also appreciate popularly written works such as op-eds for providing accessible perspectives. These informal, passive modes of information exposure are common across government structures and were frequently noted as untapped platforms, particularly among academics. Several officials also mentioned using Google regularly to find useful research and analyses.

Who is actually consuming/distilling information?

Most government officials indicated that they do not have time to seek out new cyber policy information themselves. Instead they rely on other sources / people to consume, filter, and distill information for them. The following are the most frequently mentioned sources:

- ***Trusted sources/experts (active):*** **When actively seeking information/advice, most officials primarily go to sources (people) they trust, based on past experience. These sources could be within or outside their agencies/the government.**
- ***Internal resources (mainly passive):*** **Many officials rely on someone in their agency or another agency who sends them relevant information — passively or in response to specific initiatives/events.**
- ***Key staffer (passive):*** **Some officials have a "cyber lead" (eg, a colleague, an employee, or a service) who reads new cyber policy articles and attends conferences, filters and sends them relevant or interesting information.**

3. The Cyber Policy Community Inside Government

Table 1-6 Public Sources for Cyber Policy Information and Most Frequently Mentioned Resources

SOURCES FOR CONSUMING INFORMATION	FREQUENTLY MENTIONED SOURCES
Email digests, listservs	**Policy reports:** Center for Security and International Studies' (CSIS's) "Securing Cyberspace for the 44th Presidency" (3) Zurich Insurance and Atlantic Council's[$] "Beyond Data Breaches: Global Aggregations of Cyber Risk" (2) **Threat incident reports:** Verizon (4) FireEye (3) Microsoft^ (2) McAfee (2) **Blogs & digests:** LawFare (6) Just Security (3) Foreign Policy Review (3) The Intercept (2) Volokh Conspiracy (2)
Social media—Twitter, blogs	
Popular media—opinion editorials	
Data analytic reports	
White papers, reports, journal articles	
Conferences	
Workshops, seminars, roundtables	
Individual briefings	

Note: Resources are listed based on the number of times mentioned. ^ Includes Microsoft Code Threat. $ Only Zurich's name was mentioned as the author of the report during interviews.

Intelligence and analytic reports. Those with access to intelligence data and reports rely most heavily or solely on those sources. In addition and for those without access to intelligence reports, the intelligence-heavy nature of the cyber field has led to the organic rise of a niche group: third-party mediation firms that compile and analyze data from their clients. Common examples mentioned in interviews were the annual threat reports compiled by FireEye[8]; Verizon's annual Data Breach Investigations Report[9] (in collaboration with the United States Secret Service [USSS] since 2010); and, less frequently mentioned, Microsoft's threat intelligence reports[10]. These reports are considered valuable because they fill a void by presenting trends and threats using real, anonymized data but in an open-source format that can validate government intelligence and be referenced in public forums.

Written work. Depending on the individual's purview, time, and ability to read longer works, interviewees also consume information via white papers; project reports; and, less frequently, journal articles. Although these formats are among the mostly highly used by academics, think tanks, and other research organizations, government officials find them difficult to consume for a number of reasons.

- **Reports or papers were poorly structured**, making it difficult for readers to see and consume key information. Well-formatted reports contain an executive summary and visible, strong (clearly worded) section headings. Such characteristics are highly valued for efficiency in reading.
    - One official stated that the best written input uses this structure: "You are currently facing problem X; you should use solution Y for reasons Z." Industry regularly uses this structure, but others do not.
- **Journal articles are often absent from the passive channels of communication** mentioned above. Policymakers are very rarely exposed to peer-reviewed academic work because of the time and cost required to consume this material. In some cases, staff in government agencies and legislative offices review such articles and pass relevant information up the chain, but even this approach seems to be rare.

[7] Of note, one official who confirmed this statement also commented that a lot of the intelligence comes from open-source (i.e., public) materials, such as social networks, meaning that the intelligence community does look at data from "outside sources."

[8] See here: https://www.fireeye.com/current-threats/annual-threat-report.html.

[9] See here: http://www.verizonenterprise.com/verizon-insights-lab/dbir/.

[10] See here: https://www.microsoft.com/security/portal/enterprise/threatreports.aspx.

3. The Cyber Policy Community Inside Government

- **Government officials perceive that reports and papers are more focused on theory than application.** Some agencies seek frameworks and high-level thought leadership as they grappled with issues, but most find written work to be irrelevant and nonconstructive to their decision making, written at the "30,000 foot level." Interviewees recognize that authors often lack the intent to make their work policy relevant, but government officials feel frustrated and constrained by the lack of information to help them prescribe useful solutions. As one participant noted, "We need academic rigor and rigorous analytic framework. The government policy community is also to blame. We are not articulating much about it, there is not enough raw material for academics to work with."
- **Academic writing is often very slow to be published**. Academic work can take a year or longer to be published and widely disseminated. By this point, the information therein may be of little use to policymakers. Multiple agencies noted that such delays, which primarily result from the peer-review process, are a major barrier to the usefulness of academic research.

Verbal communication is perceived as more efficient and accessible than most written work for short-term needs and for building relationships between government and external experts. Most government officials interviewed attend a number of public and private events to gain exposure to new ideas and probe deeply into topics of discourse. Participants frequently attend conferences, although many noted "conference fatigue" and stated they increasingly only attend conferences at which they are invited to speak, that have direct relevance to their current priorities, or that purport to take a novel approach to issues. They also attend public seminars, workshops, and roundtables, although their perceived value and depth vary. Many interviewees work in positions that place significant constraints on their ability to have formal communication with outside groups as quickly, frequently, or cost-effectively as they would like. These officials noted that public forums are particularly helpful and effective ways for them to communicate or test ideas before fielding formal government requests for help. Many noted the value of more private meetings that permit deeper analysis of a topic area. Although these platforms enable greater exposure to ideas, officials noted that few are outcomes oriented and progress after the event was typically limited. Suggested future

How is government sending demand signals?

A key criticism of nongovernment actors has been their lack of familiarity with government capabilities and priorities. When probed about how government agencies are conveying a "demand signal," many participants acknowledged that few formal structures existed but gave examples of informal communication strategies they employ:

- **Agencies release strategy documents highlighting priorities or agendas:**
  - **White House OSTP 2016 Research and Development Strategic Plan**
  - **Department of Defense 2015 Cyber Strategy**
  - **Cyber Command—Commander's Vision 2015**
- **Speeches at public forums**
- **Strategically organized public forums where the invited participants advance or encourage a particular agenda**
- **Closed-door meetings—can be initiated by nongovernmental organization**

Ideas from outside of government were believed to have a higher likelihood of adoption when tied to or framed in the context of government priorities.

In particular, one participant noted that policymakers often provide a lot of helpful information on their interests and needs (demand signals) in their speeches, but a person watching/listening to the speech has to listen intently; information on interests and needs often is not stated as "we need help with X."

3. The Cyber Policy Community Inside Government

Despite the value placed on one-on-one briefings and officials' openness to them, few groups other than industry seem to take advantage of this method of contact. One interviewee approximated that for every 100 requests to meet from industry, there would be 10 requests from advocacy groups and only 1 from academia.

outcomes discussed at such events include white papers, sustained partnerships, or follow-up events, all of which officials said they would find useful.

The most effective mode of communication recognized by most interviewees was **one-on-one briefings or phone calls**. Almost all of the interviewees stated that they and most other government officials are open to personal communication. In cases where they could not personally attend meetings or phone calls, staffers were typically available to participate, and if intrigued, would pass information up the chain of command. Several interviewees explicitly stated their office policy is to take all meetings requested. Personal briefings have the advantage of presenting curated information in a time-efficient and easy-uptake format. They are also an entryway for newcomers to the field, because many officials recognize the difficulty of finding the right person with whom to share information. Personal briefings expand the initial network of contacts and raise the probability of finding the correct and interested parties.

Despite the value placed on one-on-one briefings and officials' openness to them, few groups seem to take advantage of this method of contact. Academics rarely reach out to government agencies; a common perception within government is that academics would rather publish a paper than set up a briefing in Washington, DC: "After completing some research, a lot of the academics do not think in their minds, 'I need to go to DC and communicate this to somebody.'" For those seeking tenure, for example, conveying information to government officials might not be a useful way to advance their academic career.

Think tanks and advocacy organizations are more likely to perform outreach to government than academics, and industry is by far the most engaged in requesting frequent one-on-one meetings with government officials. Although the level of engagement by different groups certainly seems to vary across agencies, one interviewee approximated that for every 100 requests to meet from industry, there would be 10 requests from advocacy groups and only 1 from academia.

When nongovernmental organizations do present information via briefings or presentations, few position themselves consistently to provide actionable and constructive information. Think tanks or advocacy groups were noted as often being purely critical without offering solutions; the same groups are not always familiar with government documents, relevant laws, or an agency's mission/strategy before meetings. This broader issue of presenting policy-relevant information pertains to academics, think tanks, and advocacy organizations, who are either resistant or unprepared to present information in a manner that would aid immediate decision making. Officials recognize this issue as a challenge for both government and outside organizations.

Some suggested sharing key challenges or current policy discussions from within government to presenters before meetings or sending questions they would like answered during the presentation. Other officials find academics and others to be too resistant, on principle, to influencing policy, regardless of government outreach. Interviewees' perceptions of industry meetings varied across agencies: some find them to be direct and strategic about their presentations and demands from government, while others think their personal interests prevent them from sharing all information regarding breaches, and they instead find advocacy organizations better positioned to speak to global issues.

4.

Perceptions of the Cyber Policy Community Outside Government

4. Perceptions of the Nongovernmental Policy Community

We posed the question "What people or organizations from outside of the government influence your thinking on policy decisions?" Table 1–7 presents aggregated responses from interviewees. Responses were not restricted to refer to any one sector and naturally capture a range of interest groups, industries, academia, and others. Over half of the participants mentioned Jim Lewis or CSIS broadly, far exceeding the mentions of any other individual or group. In several other instances, participants highlighted key individuals instead of the organizations themselves; we note this in column 4 of Table 1–7. The recognition of individuals rather than organizations emerged as a pattern throughout the study, and we discuss this further in our recommendations in Section 6.

Notably, this was an exercise in immediate recall and does not purport to represent true awareness of outside parties, nor necessarily who influences thinking most strongly. Responses reflect varying interpretations of the question but nonetheless provide a high-level snapshot of organizations' presence in government consciousness.

Table 1-7 Frequently Mentioned* Organizations and Influencers

TYPE	ORGANIZATION	TOTAL MENTIONS	KEY INDIVIDUALS MENTIONED* (IF ANY)
Academia	Harvard University (incl. the Berkman and Belfer Centers)	7	Michael Sulmeyer, Joe Nye, Melissa Hathaway
Academia	Stanford (incl. the Hoover Institution)	7	Herb Lin, Amy Zegart
Academia	Carnegie Mellon University	6	
Academia	Massachusetts Institute of Technology (MIT)	5	Daniel Weitzner
Academia	University of California at Berkeley	4	
Academia	National Research Labs	3	
Academia	George Washington University	3	Orin Kerr
Academia	University of California at San Diego	2	
Academia	University of Toronto (incl. the Munk School of Global Affairs)	2	
Advocacy	Center for Democracy and Technology	9	
Advocacy	Electronic Frontier Foundation	6	
Advocacy	Chamber of Commerce	5	
Advocacy	ACLU	2	
Advocacy	Sector-specific councils	2	
Individual^	Bruce Schneier	4	
Industry	FireEye (incl. Mandiant)	4	
Industry	Crowdstrike	3	Dmitry Alperovitch, Steve Chabinsky
Other	Good Harbor Consulting	5	Richard Clarke
Think tank	Center for Security and International Studies (CSIS)	20	Jim Lewis
Think tank	Brookings Institute#	7	
Think tank	New America Foundation (incl. the Open Technology Institute [OTI])	6	Ian Wallace, Anne Marie Slaughter, Peter Singer#
Think tank	Atlantic Council	6	Jason Healey
Think tank	Center for New American Security (CNAS)	5	Richard Danzig
Think tank	RAND	4	Igor Mikolic-Torreira
Think tank	Carnegie Endowment	4	George Perkovitch
Think tank	SANS	3	
Think tank	Council of Foreign Relations	3	Rob Knake
Think tank	Heritage Foundation	2	

* Only organizations and individuals with more than one mention are included in this list. # Several government officials incorrectly believed that Peter Singer was at Brookings rather than New America; as such, the number of mentions of Brookings could overstate its influence. ^ In most cases, individuals and their organizational affiliation were mentioned; however, in one case, all mentions were only of the individual, without mention of affiliation.

4. Perceptions of the Nongovernmental Policy Community

Academia

We did not find wide dispersion in the academic institutions that government officials were aware of or accessed. Most interviewees referenced the same set of institutions, and many noted that they are not aware of the breadth of academic work occurring throughout the country at a wide variety of academic institutions; instead, they usually rely on their experience and familiarity with certain individuals or research. Carnegie Mellon, Harvard, and Stanford were noted in particular for having strong ties to government officials. Several interviewees mentioned only one of the listed academic institutions and noted it as being the only one they were very familiar with. In several cases, the official had worked at or graduated from/attended the primary institution they mentioned before becoming a government official.

Relationships with researchers at academic institutions imply stronger and more frequent communication with government, which is sometimes leveraged into roles directly influencing policy decisions. Several interviewees described, for example, involving Carnegie Mellon in short-term analyses that immediately informed a bill or policy. Policymakers are familiar with the research and capabilities of the institution and have the existing relationships to move quickly in a time- and resource-constrained environment. One interviewee recommended that universities from outside the beltway create a stronger presence in Washington, DC, through a formal structure or more frequent government briefings.

Importantly, the academic institutions mentioned have cybersecurity centers and many experts who have an interdisciplinary focus. These institutions all have cybersecurity experts with experience and/or an educational background in at least two of the following: a relevant technical area, policy, and law. Therefore, officials believe they can ask experts at these institutions questions from one perspective and receive answers that are based on a consideration of multiple perspectives. Several officials mentioned the combined breadth and depth of individuals as being a key factor in determining which experts they contact.

Although most officials mentioned engaging with one or more academic institutions regularly, academia is generally criticized for moving more slowly than other types of organizations and for being less directly concerned with influencing policy, both by design and in effect.

Some interviewees shared anecdotes of academics presenting research to them but refusing to take specific policy positions when probed for their input or feedback.

> In general, government officials tend to establish and maintain relationships with top experts in their respective fields but lack a broader understanding of the cyber research community, in particular research being conducted at less prominent institutions.

Many officials acknowledged the need for more research and thinking related to the social, economic, and political aspects of cybersecurity, because it was "no longer a technical issue." They viewed this as a long-term workforce issue, as well as a short-term need for existing research to be framed and designed as "policy relevant."

Furthermore, interviewees perceived academia as constrained to limited platforms of communication: journal articles and conference presentations. Officials noted that academic research is often written and presented in a way that requires too much time and/or expertise to interpret the results and affords little if any attention to the practical or actionable implications. Instead, officials called for using more widely accessible methods of communication, including newspaper editorials, press briefings, social media communication, and government-focused briefings. Many officials suggested that for research projects having policy implications academics should develop 1- to 2-page policy briefs summarizing the methods used and key results, providing a clear description of the relevance to policymakers and offering specific recommendations.

In general, government officials tend to establish and maintain relationships with top experts in their respective fields but lack a broader understanding of the cyber research community, in particular research being conducted at less prominent institutions. This lack of broad knowledge is likely due to supply and demand constraints. On the supply side, many academics are ineffective in their outreach and communication to policymakers, rarely highlighting policy-relevant research results. On the demand side, government officials seldom take the time to communicate their needs to academics, nor do they spend the time networking with or reading research by a broad set of experts; as a result, officials usually neglect research outside their fields of expertise.

Think Tanks

Degrees of Influence: The Role of Jim Lewis

When government officials were asked whom they listen to outside government on cyber policy issues, Dr. James (Jim) Lewis, Senior Vice President and Program Director at CSIS was mentioned nearly universally. Many participants noted that they have great respect for Lewis, and even more noted that he plays a significant and important role in cyber policymaking. However, several officials noted that they often privately disagree with Lewis's viewpoints and that his formidable influence in government cyber policy may make it difficult for other, less well-connected voices to be heard.

Based on our interviews, Lewis' prominent role in government cyber policymaking is likely the result of a variety of factors -- he meets very frequently with government officials, listens to their needs, and then provided relevant information from the private sector and develops ideas to help solve specific problems.

Lewis previously worked in the U.S. State and Commerce Departments and has extensive experience in political, military, and security realms, including as a negotiator. Since leaving government, he has stayed in contact with government officials working on security topics, especially those related to cyber. Lewis uses his contacts to help facilitate information sharing and knowledge building among stakeholders.

One participant characterized Lewis's role as providing a "critical mechanism to facilitate information flow into and out of government." When he speaks publically, his comments are often perceived as representing the views of government officials whose official voice may be restricted. Separately, he meets with private-sector participants and communicates their views and his analysis back to key government stakeholders.

During an on-the-record interview for this study, Lewis provided some insight into how he operates. Lewis takes a broad view of "cyber" and values lessons he has learned from noncyber areas that can be applied to cyber when conducting analysis, interpreting findings, or suggesting policy. Lewis focuses his attention on consuming and producing information that has clear value to specific groups and information that meets one or all of the following criteria: is based on primary data, is countable and verifiable, and offers radically new insights.

Lewis highly values communication—both soliciting information that acts as critical input to inform and focus his work and sharing his ideas—to ensure the work that he conducts leaves an impact. Lewis is a prolific communicator, believing that "you need to do it all" in terms of participation and idea dissemination: sit on panels, participate in public convenings, publish, be quoted in the media, participate in private or informal events, and act as an observer. Lewis focuses on high-quality communication venues, noting that he prefers to share ideas through verbal discussions. As a result, he no longer uses social media (such as Twitter), and he tends to eschew most conferences. Even when no forum is provided, Lewis tries to be proactive, offering his perspective and input on topics or trends that he believes are critical: he will often email contacts in government titling the subject line "Unwanted Advice."

Lewis's leadership and influence are widely believed to be unparalleled by virtue of both his ability to build consensus on particularly challenging cyber policy issues and the efficiency and effectiveness of his communications with so many audiences.

4. Perceptions of the Nongovernmental Policy Community

All government officials noted awareness of and some engagement with at least a few think tanks focused on cyber policy, primarily think tanks based in or with a significant presence in the DC area. Of those that were most commonly recalled, CSIS is a clear leader, mentioned by 20 officials. The remainder of the list of think tanks mentioned reflects many organizations that are perceived as thought leaders across many sectors and policy topics in DC.

When asked what drew government officials to each think tank, officials offered several reasons. In general, officials are more interested in engaging with specific individuals, rather than with certain organizations. If "good people" left an organization, officials do not feel tethered to the organization.

Of particular note, many officials recognized Jim Lewis as being key to CSIS's prominence and success. As one interviewee stated, "I don't know about CSIS, but I know Jim. Jim is always someone you want on your team." Lewis, in particular, was recognized for holding influence across the cybersecurity community. Several officials highlighted CSIS's and Lewis's power to convene industry and government officials on cyber policy topics and CSIS's ability to convene such groups on a wide variety of policy topics, cyber and otherwise.

Organizationally, several officials mentioned New America and discussed its innovative programming and recent acquisition of cyber thought leaders. More than any other think tank, New America seemed to be recognized as valuable for both the individuals working there and the organizational leadership and its unique focus on topics often neglected by others.

Other important factors included think tanks' sustained interest and experience in cyber. Officials usually value opinions of individuals who have worked on cyber-related topics for many years and often shun newcomers to the space, whom they felt revealed their limited knowledge in written work and other communications. However, several officials noted that policymakers often reject entirely new and more transformational ideas because they are too challenging to implement; more incremental ideas can be adopted more quickly and easily.

Finding the balance between incremental, pragmatic ideas and new, more transformative solutions to a given problem seems to be a challenge faced by think tanks and policymakers alike. One interviewee noted that a third focus area for think tanks and others should be developing new ways to communicate old and new ideas to different audiences, possibly resulting in a change in one or more stakeholder groups' perspectives.

A think tank's past government experience is also highly valued, based on a pervasive sentiment that few individuals outside government truly understand its decision-making process and constraints. As a result, think tank output is often perceived as not sufficiently solution oriented or constructive and as ignorant of the resource and process constraints affecting government agencies. "Good" individuals within think tanks effectively address these concerns by either ascertaining buy-in from the intended government consumer before conducting a study, directly asking about current needs and priorities, or presenting novel ideas supported by data.

Think tanks are valued for their convening power, which was praised by many officials we interviewed. Several officials noted that CSIS and other think tanks play key roles in developing cyber policies such as the NIST Cybersecurity Framework and CISA, by bringing together government, industry, academics, and other stakeholders. Input from these gatherings fed into the policy development process and subsequently ensured greater buy-in from nongovernment organizations, industry in particular, during implementation. The perceived need for convenings led by nongovernment organizations varies across agencies, however, because some government agencies are better positioned or inclined to assemble stakeholder gatherings themselves.

Advocacy Organizations

Interviewees mentioned advocacy organizations as often as academic institutions when asked about organizations that influence policy decisions. However, when advocacy organizations were mentioned, the name of the organization was the focus of interest for officials, rather than one or more specific individuals being the primary focus, as was the case with academia and think tanks. Most officials listed at least one advocacy organization as being helpful in cyber policy debates, and officials had widespread awareness of a core group of advocacy organizations, including those listed in Table 6. Multiple officials also identified other lobbying groups directly related to their area of work.

4. Perceptions of the Nongovernmental Policy Community

> "Not too many people think about building consensus … People are putting out ideas on one side of the debate, trying to pull people to them. Not as many trying to find a way forward after the debate is already put out."
>
> *– A former White House official*

The Center for Democracy and Technology, the Electronic Frontier Foundation, and Chamber of Commerce appear to be most influential and "most useful on their issues." One official mentioned an advocacy organization that works solely on his agency's issues and is very effective in supporting and influencing cyber policy debates in which that agency was a key stakeholder.

Despite widespread awareness of advocacy organizations, officials' perceptions of value added by these organizations vary by agency and context. Several participants find engaging advocacy organizations that represent broader constituent groups, including industry, useful during the policymaking process to ensure early buy-in for any proposed legislation or policy. Reasons for engaging these organizations vary between providing a rubber stamp approval on a policy and providing insights affecting its development. Others, however, said several organizations—in particular the Chamber of Commerce—are ill informed on issues, fail to add a constructive voice to the policy conversation, and sometimes derail the policymaking process. One participant shared an example of a generic letter to Congress issued by the Chamber of Commerce during discussions about CISA that unintentionally instigated reactions among the privacy and civil liberties communities.

Our interviewees' perceptions about advocacy organizations' ability to communicate with policymakers also vary. Some appreciated the direct "asks" that advocacy organizations tend to make or their ability to share information regarding their constituents that individuals or companies may not be positioned to reveal. Others felt that advocacy groups do not have a strong base of technical subject matter experts. Several government officials noted that they find establishing a "common language" with advocacy organizations to be difficult, primarily because advocacy organizations are often only interested in discussing a singular topic within a broader policy topic being debated.

In general, policymakers tend to engage frequently with advocacy organizations, largely in response to a request by the outside organization itself. Officials tend to be aware of the biases inherent in arguments and information presented by single-issue organizations but feel nonetheless equipped to continue sharing information given the important stakeholders they represent. The strongest recommendations offered by several officials for advocacy organizations are to better understand the policy context and to improve technical proficiency, in order to enable them to lend more useful and thus more influential voices to policy conversations.

Comparing Impressions of Nongovernmental Organizations

Broadly, our interviews suggest that many government officials perceive different groups outside government in very traditional ways: academics are viewed as conducting mainly conceptual research, in contrast to industry representatives who are very focused on applied issues, and think tanks are somewhere in between. In terms of bias, academics are generally perceived as being the most objective, think tanks are considered equally as objective in most but not all cases (several officials noted that think tanks may be influenced too much by government or by industry, resulting in fewer new/provocative ideas), and industry is perceived as being the most biased.

Government officials did have some differing opinions about academics, and several government officials noted that while they perceived academics as the most objective group of cyber policy experts outside government—as compared to industry, advocacy groups and even think tanks, all of which appear to have more obvious biases/financial motivations—they still see many academics as biased, based on personal versus institutional beliefs.

As introduced above, some academics and individuals at think tanks—particularly newcomers to the field—are seen as frequently regurgitating old ideas. Academics are widely seen as prioritizing publishing their

[11] Of note, individuals outside government face a tension between offering policy recommendations that are aligned with current government programs and strategy and thus are likely to be more actionable (eg, easier to adopt), versus ideas that are new and more provocative, which may not be adopted as quickly or easily.

4. Perceptions of the Nongovernmental Policy Community

Academics are perceived as moving very slowly, too slowly for the needs of government initiatives. However, many individuals mentioned that academics serve a very useful role by helping develop critical intellectual capital that is needed in the cyber policy community.

research over conducting research helpful to government stakeholders or communicating with the government; furthermore, academics are perceived to move very slowly, too slowly for the needs of government initiatives.

Importantly, however, many individuals mentioned that academics serve a very useful role by helping develop critical intellectual capital that is needed in the cyber policy community. Although the officials who seemed most supportive of the current role played by academics had themselves worked in academia at some point in their careers, our interviews did not explicitly ask officials about the value they place on more conceptual and theoretical research being done by academics and others. The discussions in which this topic arose suggest that many, if not most, government officials are not opposed to academic research, but they have a strong desire for additional research that is more applied.

Many officials asked for more research that focuses on either specific policy options being discussed inside government or policy options that are more grounded in the current or near-term political environment. Others asked for more research that aims to connect basic, conceptual, and theoretical research to practical applications, through additional analysis and clearer communication.

How do government officials decide who to listen to?

Several key factors emerged as very important to many or most government stakeholders in deciding when to read a paper, attend a conference, or meet with someone:

- **Is the information coming from a trusted source (individual)?**
- **Is the organization known for high-quality work (i.e., a strong brand)?**
- **Do they have a positive impression of the author (through past experience)?**
- **Does the information include new data?**
- **Does the information appear to be from a different angle?**
- **Does the person have a security clearance?**
- **Does the event offer an opportunity to engage in a unique discussion (e.g., private events hosted by a think tank)?**

5.
Barriers and Enablers to Cyber Policymaking

5. Barriers and Enablers in Cyber Policy

> "Most [elected] members of Congress do not use computers or email. Key agency Secretaries didn't know how to use email. At the top level! The education piece alone, getting them 'baselined' enough to have and understand [cyber] discussions, takes months."

Cyber policy is still relatively new and not entirely understood by those in government policymaking or policy-influencing positions. As pointed out in previous scholarship on this topic, the definition of "cyber policy"—or lack thereof—causes much disagreement, consternation, and confusion. As one participant described cyber, "It's a cross-cutting issue; no clear place to begin, with no clear solution." Because cyber policy is ill defined, describing it was challenging even for the purposes of this research study.

Lack of High Quality, Relevant Data

Quality open-source data related to "cyber" events are challenging to obtain. The highest-quality data from some cybersecurity problems are being collected by the holders of critical infrastructure in this space (i.e., private industry); however, according to government officials and others interviewed outside government, these data are rarely released by the owning organization or aggregated by the private sector without public-sector involvement. Intelligence sources within government can access some of this data, but in most cases, they are unable to openly publish or share much, if any, of it. According to one official, "Cyber is so new, it's not fully thought through. It's the only set of crimes where reporting to the government is a fraction of a percent, and that's perceived as okay." When asked about key barriers to cyber policy, many officials mentioned the critical need for more and better data and answers to questions such as the following: "How do you measure cybersecurity?" "How would you measure progress?" "What are effective and measurable outcome metrics?" "How do you explain the benefits of every additional dollar of cybersecurity?" These questions are all high priorities within government, but clear answers or solutions do not seem near at hand.

Insufficient Understanding of Cyber by Key Government Officials and Staff

Government participants involved in cyber policy most often cited government policymakers' and influencers' lack of knowledge as the primary barrier in being able to craft effective cyber-related policies and legislation. "Most [elected] members of Congress do not use computers or email. Key agency Secretaries didn't know how to use email. At the top level! The education piece alone, getting them 'baselined' enough to have and understand [cyber] discussions, takes months."Another participant described a series of efforts to educate Congress—it involved over two dozen different hearings and closed-door briefings to get policymakers comfortable enough on the issues to even begin considering legislation. Yet, concern over the lack of cyber knowledge in Congress remains because of staff turnover, despite this "enormous investment" of energy and resources. Outside of Congress, many government officials are also perceived to lack knowledge to make good cyber policy decisions, although our interviews suggest the level of knowledge has increased in the last several years.

> The difference in perception offered by interview participants appears to align with how political one's position was—that is, the closer to the legislative decision-making process the participant is, the less likely the participant felt it is important to have technical experience.

Participants all agreed that government officials and members of Congress need to be at least conversant on the issues surrounding cyber policy; however, *interview participants were divided over the importance of having a technical background*. Some felt that it is essential, while others felt that it is far from necessary. Several participants also noted that officials with a technical background can sometimes be blinded from considering other nontechnical factors when reviewing a cyber policy issue. The difference in perception offered by interview participants appears to align with how political one's position was—that is, the closer to the legislative decision-making process the participant is, the less likely the participant felt it is important to have technical experience.Instead, the individuals at this end of the spectrum tend to value political savvy over technical know-how. Several officials who lack technical knowledge themselves noted the importance of having access to a trusted and responsive technical resource who could answer questions or is

5. Barriers and Enablers in Cyber Policy

willing to dispense knowledge and opinions; however, one official did note the difficulty in assessing the quality of the technical information and guidance they receive.

Legal Restrictions on Information Sharing

Complicating any discussion about cyber is whether individuals within and outside of government can speak about it at a classified level. If restricted to addressing it at nonclassified levels, discussions can be so vague that they border on useless. Government policymakers and influencers who have been given access to intelligence products reported that those products typically provide more value than other publicly released research reports and data, primarily because the data on which the reports are based are considered richer and more robust. However, several officials noted that many government officials, particularly lawmakers in Congress, often overvalue such data. Meanwhile, most academics and think tank researchers are blind to these data, which includes primary data from intelligence, law enforcement, and corporations.

Interviewees mentioned other government laws as barriers to discussing policy-related topics with individuals and organizations outside of government. The majority of government officials interviewed noted that they highly value engaging in informal policy discussions and sharing information with members of the nongovernment cyber policy community. However, government officials are restricted from engaging in such ad hoc meetings that are not open to the public if one or both of two primary conditions are true—if the official is fully or partially responsible for developing new policies and if a specific policy is being discussed or debated officially (i.e., will potentially result in a new policy document, such as a Congressional bill or an executive order). These restrictions are based on federal open meeting law, such as the Federal Advisory Committee Act (FACA), and other restrictive statutory schemes; several officials' perceptions of these restrictions made them hesitant to even mention that such meetings occur.

The intention of legislation restricting meetings is to promote a transparent government and increase agency accountability, yet such interaction is essential for learning and developing fresh ideas and perspectives, especially when an area is so new and potentially complex as cyber. One official noted that he and other officials directly responsible for policy development do regularly engage in informal discussions with external members of the cyber policy community, but that when he does so, he does not discuss specific policies under current or potential future consideration.

Cultural Norms

The culture of government can work against it in establishing policy, in particular in Congress. Several officials noted that government broadly has become more reactive in its stance; one official noted this as a significant change over the last 50 or 60 years. Further, several individuals outside of government stated that government is usually very slow to enact new cyber-related laws and regulations, which significantly lag behind technology advances. As a result, laws in this area need to be written that are durable and should consider how technology is evolving and affecting various stakeholders before legislation is passed. Compounding the problem, it can often take years for new legislation to pass (for example, CISA).

The culture of academia (and think tanks that are sometimes viewed as quasi-academic) often works counter to effectively communicating research results to policymakers or to conducting research that policymakers see as valuable. Academics are interested in and incentivized by their institutions to focus on research topics that are less applied and to publish their results in peer-reviewed publications. For a certain piece of information or finding to make its way successfully into government usually takes a lot of extra work and advocacy—more steps need to happen beyond those for which academics are rewarded. Further compounding the challenge of academic research results reaching policymakers, the peer-review process can often take many months or even years. If a finding is published 6 months to a year after the research is completed, the value of the finding, which could focus on a specific cyber event, may be significantly lower, even if it independently confirms what popular thought had been at the time. Many government agencies need to be able to act (or react) the moment a cyber event is suspected, rather than up to a year later. Finally, there is a perception that academia can be biased on certain topics. The culture of academia promotes availability of information and scholarly thought. When considering intellectual property literature (as it relates to cyber, such as the Digital Millennium Copyright Act), it would be challenging to find academic articles encouraging *stronger* copyright protections. It simply is not part of academia's normative culture.

5. Barriers and Enablers in Cyber Policy

> "We sometimes hear an academic recommend that 'the U.S. government should secure cyberspace.' What does that mean? It needs to be more specific and more actionable."

According to many government officials, researchers often do not understand government structures or processes, so they make recommendations that are too theoretical, disjointed, or simply unreasonable. Several officials also stated that academics often offer recommendations that are "too high level and abstract"; one official noted that academics lacking uniformed military experience are particularly guilty of this. Such a lack of detail and specificity creates a challenge when policymakers need to translate recommendations into actionable policy. "We sometimes hear an academic recommend that 'the U.S. government should secure cyberspace.' What does that mean? It needs to be more specific and more actionable."

Officials also noted that to provide helpful research and recommendations for government, researchers may need to understand topics such as existing U.S. and international laws and even cultural factors. For example, if a researcher is analyzing how the United States should react to a cyber event attributed to China, knowledge and consideration of relevant U.S.–Chinese agreements and treaties and of the structure and history of the Chinese government and domestic law enforcement, among many other factors, would be critical. Otherwise, any recommendations, although well intended, would likely be worthless.

Technologists were criticized by several officials, who commented that many individuals outside government and some inside government who are technical cybersecurity experts sometimes try to "dabble in cyber-related criminal law" without taking the time to understand it. As one official noted, "Not all technologists know what it takes to get a federal search warrant. We all talk past one another. At [conferences], some people use [legal] phrases incorrectly," which affects not only their credibility but negates any consideration of the rest of the discussion.

> Several participants also commented that the using analogies in cyber is to its detriment; it is not helpful in driving conversation and understanding. Comparisons to a "lockbox" or "unbreakable safe" can make good soundbites, but they are not helpful in providing the correct perspective.

Those in academia and think tanks may propose ideas that have been tried before, which simply recreates the wheel. "A criticism I have against universities in particular and some think tanks is that they have no understanding of what is actually going on. Unbelievably! I'm not defending what the government is doing, but you have to pay attention to what has already been tried! Maybe … you're not solving a problem that actually needs to be solved …! People [who have been] in government forget that progress continues after they have left." One example is that researchers "often recommend 'industry-driven standards endorsed by government.' Well, they have just described the NIST Framework [which has existed for several years]."

Perceptions of Academic and Quasi-Academic Research and Publications

Policymakers were also clear on what they found particularly helpful: information and ideas that are new, different, actionable, and clear and offer "smart angles." Researchers are advised to use primary data sources; have countable, verifiable data; and derive unique insights. "How we collect data is changing. The cyber community needs to think more strategically and creatively about the types of data that we collect, the data collection and analysis methods we use, and the highest priority data to collect for different analysis purposes. Cyber needs more innovative applications of methods to understand threats and predict what's coming, in the context of what the U.S. needs.

Moreover, many participants expressed a need for more rigorous methodological frameworks to be used for cyber-related research, evaluation, and other types of analyses. One

5. Barriers and Enablers in Cyber Policy

"Right now, I am overwhelmed by information. How do you filter it? Auto-sorting is over-rated and cannot be relied upon. The most consistent thing you can rely on is the information's or product's source, [whose credibility consists of] … reputation and relative experience…."

official stated, "If I can tell you the conclusion of a research report from simply reading the introduction, then I don't consider the results to be credible." Several officials thought much academic research is biased, with one official stating, "More intellectual integrity is needed in academic work." And while repetition of old ideas was frowned on, participants noted that if researchers are going to "cannibalize old ideas that did not go anywhere," then at least offer a new spin, a new perspective on the topic.

Several participants also commented that the using analogies in cyber is to its detriment; it is not helpful in driving conversation and understanding. Comparisons to a "lockbox" or "unbreakable safe" can make good soundbites, but they are not helpful in providing the correct perspective: cyber has some similarities to other issues, but many differences. Those commonalities and differences should be described instead of trying to compare them against something they are not.

Multiple government participants are concerned that too many people are joining the fracas just to be critical or to grandstand. Such individuals are often viewed as not making meaningful and constructive contributions but rather are trying to make a name for themselves. Several officials stated that revered individuals from other fields are delving into cyber and are too casually being published in op-eds. Two former senior government officials specifically named in this context were Joe Nye and Richard Danzig, both of whom frequently write and speak on a variety of public policy issues, and are in senior government were both named specifically in this context.[12] Officials espousing this viewpoint noted that such individuals are creating little value for the cyber policy community and instead are merely adding to the "noise" of cyber policy reports and opinions. However, other government officials spoke very highly of the value that Joe Nye and Richard Danzig have brought to the cyber policy debate, specifically noting their knowledge of government and ability to convene people with divergent viewpoints and help find common ground.

Almost all of the government officials we interviewed posed this challenge: How to separate the signal from the noise? "Right now, I am overwhelmed by information. How do you filter it? Auto-sorting is over-rated and cannot be relied upon. The most consistent thing you can rely on is the information's or product's source, [whose credibility consists of] … reputation and relative experience…."

[12] Nye is an esteemed Harvard professor who served as Charmain of the National Intelligence Council under President Clinton, an Danzig served as the Secretary of the Navy under President Clinton and has wide-ranging legal and policy experience.

6. Conclusions and Recommendations

6. Conclusions and Recommendations

6.1 For the Hewlett Foundation and Other Funders

The Hewlett Foundation and other funders should find a significant amount of useful information in this demand assessment conducted with government stakeholders. Through its Cyber Initiative, the Hewlett Foundation is attempting to improve the supply of new ideas, tools, data, and other sources to support the cyber policy community. A better understanding of one of the largest groups of intended beneficiaries or users, the U.S. government, provides critical insights that can help the Foundation and others with shared aims to ensure that their investment results in "products" that are reviewed/consumed and, ideally, adopted and used by one or more government stakeholders.

From this vantage point, we recommend that the Foundation critically review all of the recommendations below for academia, think tanks, and U.S. government stakeholders, all of which could help guide their investments to be more useful to the government and the cyber policy community broadly. More specifically, we recommend that the Foundation engage in the following broad activities as much and as often as possible:

1. *Talk with key government officials (and other intended stakeholders/beneficiaries) as much as possible*—Ask them about their priorities and what they want/need currently and in the near term and use the information gleaned to help select grants and disseminate results of ongoing or completed grants.
2. *Push grantees to clearly describe the intended audience(s) and impact(s) of their research and/or provide stakeholder engagement support to grantees*—Grantees should provide as much detail as possible on who will benefit directly and indirectly from their research and explicitly how they will benefit. The Foundation should review these plans and decide to fund grants based in part on these plans. Or the Foundation could offer additional support to grantees to help with stakeholder engagement. Note, this suggestion does not mean that all cyber policy work should necessarily be applied in nature but that potential longer-term implications and applications should be explored as early as possible.
3. *Push grantees to engage more with government*—If government is one of a grantee's intended key stakeholders, the Foundation should push the grantee to propose engagement with one or more government agencies before, during, and after the project, if possible.[13]

In addition, the following list of recommendations for the Foundation and other funders is based on comments made by one or more government officials:

- *Push industry to play a more objective role*—Industry almost always communicates to government why a new policy or regulation will hurt them; rarely do members of industry attempt to propose or support efforts that seem objectively aimed at improving cyber policy.
  - Example: The Foundation could work with insurance companies to help bolster the role they could play in the future.
  - Example: The Foundation could work with a variety of industry sectors to identify ways that academics and other members of civil society could make greater use of certain industry data sets.
- *Engage more people with new ideas*—Several government officials commented that entirely new ideas are very rare. The people who are serving on various government commissions and some of the individuals who have been given grants by the Foundation tend to be the same people, recycling the same ideas. Whether they have been involved in cybersecurity for years and are repeating the same ideas or they are new to cybersecurity and are repeating the same ideas that the cyber community discussed but set aside for specific reasons, entirely new ideas are rare.
- *Support the development of more data specifically aimed at helping compare costs vs. benefits of various initiatives/policy proposals*—When regulations are debated, data come almost exclusively from industry. When national security topics are discussed, data come almost exclusively from the NSA, etc. The Office of Technology Assessment used to play a more objective role for Congress, but it was shut down in 1995. Since then, agencies have generally played this role themselves; the U.S. Environmental Protection

[13] Importantly, as noted elsewhere in this report, there is a clear role, supported by many of the officials interviewed in this study, for academics and others to develop ideas that government officials do not ask for; however, such research may not be directly useful to policymakers, particularly in the short term. Additional engagement with government by some members of the cyber policy community could help more cyber policy research directly influence near-term cyber policymaking.

6. Conclusions and Recommendations

Agency, Department of Energy, and Department of Health and Human Services conduct many cost-benefit analyses to support their work. Because of the cross-agency nature of cyber, cost-benefit analyses are not conducted for cyber. Several interviewees suggested that Hewlett support efforts to fill this gap.

- *Promote increased cyber education for policymakers*—Focus more on ways to increase high-level policymakers' understanding of cyber issues to a baseline to allow them to engage more in discussions.
- *Promote increased public education, recognizing the critical role of the media*—Without more public understanding of and support for cyber topics, policymakers will find it difficult to make significant cyber policy changes; and the central role that the media plays in what the public understands about cyber cannot be overstated. Several interviewees noted that Hewlett should focus more attention/funding on this area, for example, by encouraging grantees to engage more with the media and supporting media efforts aimed at educating the public.
- *Help identify/create and support new venues for specially designed academic/think tank publications with policy audiences in mind*—For example, the recently launched *Journal of Cyber Policy* and the *Journal of Cybersecurity* are trying to provide strict requirements, not simply op-eds, and to serve as focal points that enable more publication of interdisciplinary cyber policy research of interest to policymakers. But to be relevant to policy, the articles need to be crisp, concise, and written for a policy audience—more like Foreign Affairs than academic journals.
- *Help create and support a mechanism for groups outside government to better learn about government's priorities*—The Foundation could help facilitate information sharing on what is happening inside government by supporting a new "portal" of some sort or by sharing information on what the Foundation knows/hears through its engagement with government.

6.2 For Civil Society Organizations

Academics, think tanks, and other members of civil society should be able to learn a great deal from the results of this study by reviewing our analysis of how cyber policymaking in the U.S. government works today; what organizations outside of government are having an impact; and how government cyber policymakers decide who to listen to, what to read, and what events to attend. Some of the key takeaways from our analysis are as follows:

- *Trust is very important*—Government cyber policy officials look to people they trust (frequently and usually as an initial source) to provide high-quality, relevant input/feedback and to be discrete. Trust is established through collegiality, consistently good work, and openness/truthfulness about one's interests when presenting information.
- *Individuals matter more than organizations, most of the time*—Government officials look to individuals more than institutions when seeking information. Important individuals tend to be at organizations with strong reputations; however, if they leave, the organizations may not continue to play a role in cyber policy.
- *Organizations with a strong brand and a reputation for high-quality work get more attention*—Although individuals matter more, government officials do read/listen to unknown individuals. In these cases, they pay more attention to individuals working at very well-respected institutions. Furthermore, government often contacts organizations with strong brands for broad engagement to host an event, for example.
- *Past experience in government matters*—The typical hierarchy of information consumption is as follows: (1) others inside government, (2) people outside government who have government experience, and (3) people outside government without government experience. Government officials pay more attention to people who have government experience, as a signal that they are more likely to bring a perspective that is grounded in reality. Organizations that do not employ individuals with past government experience have been successful by partnering with individuals with such experience before engaging with government.
- *Past experience working on cybersecurity matters, but not always*—Individuals without experience working on cybersecurity are perceived with caution at first by many in government because some such individuals have presented old ideas or are not sufficiently knowledgeable about technical or policy issues related to cyber to add value. That said, many government officials said they do value new people working on cyber, when they take the time to get up to speed on the details of cyber and past work, often through partnering with others with such experience.

6. Conclusions and Recommendations

- *New data are in high demand*—Government officials are looking for new information to help make better decisions, so government is very interested in talking to organizations that offer to create and/or share new data on a relevant topic.
- *More relevant work is needed*—Government officials want research and input that are directly relevant to the issues they are working on, provide information on new options or help to compare options, and are grounded in an understanding of how government works.
- *More applied work is needed*—Government officials are very interested in nontechnical research on cyber (e.g., economics, policy, legal, and other social science–based research), but they are particularly interested in studies that use or create empirical data.
- *New ideas/perspectives are in high demand*—Many government officials are looking for people with new ideas and perspectives, rather than a rehashing of old ideas or repeating ideas already in the discussion (although this is certainly not the case for all government officials). Newness by itself, however, does not guarantee policymaker interest if it is not actionable.
- *Security clearances really matter, sometimes*—Engaging in cyber policy discussions, including with DoD, NSC, and the intelligence community, sometimes requires security clearances before government officials can provide people with enough information for them to do useful work.[14]
- *Private discussions can allow more direct discussions*—Government officials often have private one-on-one meetings and participate in private events (e.g., hosted by universities and think tanks) that bring together key stakeholders, and these types of events can enable significant collaborative progress not possible in more public forums.
- *Customized presentations are very well received*—Universities and think tanks have information that government agencies and officials therein do not. Government officials value external data and the perspectives of individuals to which they do not have access, and those outside government who present valuable data are lauded. Also, information exchange is a two-way street; providing targeted data to government officials may result in officials presenting data as well.

Members of civil society who want to have more of an impact on government policymaking—directly or even indirectly—should use the takeaways and all of our findings to consider whether and how they can help improve the disconnect between the demand for cyber policy information and the supply of such by making changes on the supply side. To have more of a direct impact on government policymaking, organizations outside of the government should design research and output to be actionable and constructive if intended for immediate implementation (as opposed to broader thought leadership or more conceptual research), and they should contextualize their work as it relates to the current policy dialogue and be prepared to discuss the implications and specific uses of their results. On the next page is a list of specific actions that we recommend members of civil society consider using each time they explore new areas of research or analysis. Taking these steps should their work be more directly useful to and/or understood by government stakeholders.

6.3 For the U.S. Federal Government

Although not one of the primary intended beneficiaries of this study, government stakeholders could benefit from reviewing the results of this study and using them as input and feedback on the role they play in the market for cyber policy information. In particular, government cyber policy decision makers and influencers should consider whether they can help improve the disconnect between the demand for cyber policy information and the supply of such by making changes on the demand side. The following are such recommendations.

1. *Communicate your needs as clearly and widely as possible*—Based on our interviews with government stakeholders, individuals in government do not read or find useful much of the work conducted by the policy community outside of government. One reason for this is that individuals outside of government do not know what cyber officials inside government want. In many cases, legal, security, and political factors restrict the ability of government stakeholders to state publicly what they are working on or what specific data, tools, or other resources would be useful with sufficient context. However, in many cases, government officials could share more information that

[14] Obviously, individuals with new ideas and perspectives often will not have security clearances, so it is important to consider as soon as possible whether these individuals might need security clearances to have the desired impact. It is possible to grant short term clearances for specific discussions and government should take advantage of this authority more frequently than it does now.

6. Conclusions and Recommendations

Checklist for Civil Society: Engaging with Government

Before beginning to work on a new idea:

1. Consider which government agency(ies) might be interested in your past work or new work that you are considering initiating/proposing to funders.
2. Contact the agencies and try to find out more about what they are working on and their current and near-term priorities, describe your areas of focus, and look for intersections/ask how you can help.
3. Use the information you glean to revise your plans as appropriate.

Before starting a new project that has been designed:

1. Consider which government agency(ies) might be interested in new work that you are considering initiating/proposing to funders.
2. Review easily accessible public information on what the government is working on related to your topic.
3. Read past work on your topic—has work already been done/published? Has government already considered doing what you are proposing but decided not to?
4. Contact the main government agency that you think will be interested or several government agencies.

After a project has been started:

1. Consider whether you could benefit from input or feedback from the government during your project, and if so, at what stage(s).
2. Consider whether you think one or more government officials could benefit from hearing how your project is going midway through, and if so, at what stage(s).
3. If you see a benefit to your work and/or for the government, contact government officials as appropriate to provide updates and/or ask for their input and feedback.

After a project has been completed:

1. Consider/revisit which government agency(ies) might be interested in your results.
2. Publish your work in journals, write and post reports/white papers and present at conferences (although few government officials have the time to read journal articles or white papers, attend conferences or read proceedings, their staff often do and further, detailed reports and journal articles and the peer-review process itself can add useful depth of information and credibility to the authors).
3. Use mediums such as op-eds, informal briefings to agencies, and blog posts. Consider maintaining social media accounts (e.g., Twitter) to engage regularly with government officials as a way to help establish relationships and a brand.
4. Develop a short (e.g., 1-page) summary of your results and what they mean for the government and other stakeholders (tailor one of these for different groups if needed).
5. Contact the government agencies likely to be most interested in your results and send them a 1-page summary, links to papers and presentations, and if possible, set up a time to meet in person or discuss your results by phone.

6. Conclusions and Recommendations

individuals outside of government could use who want to conduct research and analyses that are most useful to some or many parts of the government. Here are some more specific suggestions:

- Establish formal and well-publicized structures for communication with nongovernment organizations, including the following:
  - Identify key points of contact and recommended communication processes.
  - State whether your agency funds research/analysis by external groups and, if so, what types.
  - Describe how your agency consumes research/policy work to help outside organizations know how best to disseminate their results.
  - FACA need not be an obstacle; its intent was to provide "sunshine" on meetings, not to prevent meetings, and officials have ways to meet with outsiders that are consistent with FACA.
- Talk at conferences and post information on the internet (if possible) describing your needs or, when constraints exist, communicate as much as possible to as many people as possible.
- Be as clear and direct as possible about your needs—Describe the specific issues you are working on, the challenges you face, what you need, and what the information you seek will be used for (and why it is important).
- Offer to meet with individuals who want to help address your needs/challenges—before they start a new project and, when possible, while the project is ongoing and after the project is completed.
- Publish/post strategy and priority documents publicly if not already doing so.

2. *Provide more funding or find and help other funders*—If the government wants more applied research and analysis that is better targeted at current/immediate challenges and priorities, funding must be made available. However, many government agencies find it very difficult to request and receive additional resources to fund new research, analyses, and events. We encourage government stakeholders to consider how they can help support such work through requesting more funding for their agency/group, sharing ideas with others in government who may have funds available, and reaching out to foundations (such as the Hewlett Foundation and the MacArthur Foundation) and other civil society and private-sector organizations and individuals who may be able to self-fund their work to communicate needs.

   We frequently heard that agencies were given a responsibility within cyber without any funding to carry it out. We encourage the White House and Congress to recognize this challenge and help provide funding when requesting cyber-related work be done—Attach new funding to new policies and laws/regulations that are passed.

3. *Encourage and enable greater exchange of expertise across sectors*—This study provided further evidence of widespread interest in and need for more exchange among academia, the private sector, and government to reduce the siloes across these sectors and improve cyber policy inside and outside of the government. We encourage government stakeholders to support current efforts and look for new ways to expand collaboration and information sharing, for example, by identifying ways that current government staff can work more directly with academics and private-sector organizations and by using relationships with former government staff working in the private sector or academia.

The following are two very specific recommendations gleaned from our interviews:

- *Consider expanding fellowship programs, possibly increasing the length*—Fellowships can be very useful ways to pull information/capabilities from outside into the government. They also help transfer information on how government works and the needs (demand) of government to individuals outside government, particularly when these fellows leave government. In addition, they support the creation of new trusted relationships with government officials, many which endure after the fellowships end. Further, longer fellowship stints could add additional value, particularly given the ramp-up time needed to understand government processes and develop rapport with government colleagues.
- *Consider ways to retain institutional knowledge*—Frequent turnover of government employees with a clear understanding of cyber issues, often because of significantly more lucrative private-sector salaries, is a major problem across the government. New strategies and initiatives to retain more institutional knowledge when employees leave are desperately needed, as are broader efforts to keep more of these employees in government.

Demand for Cyber Policy Resources: State Governments

Volume 2

1. Introduction

1. Introduction

Although Washington, DC, is the primary location where government conversations about cyber policy have been occurring, it is certainly not the only location. A number of states have been debating and forming cyber policy frameworks, enacting new laws, and expanding resources, although these efforts are relatively nascent compared with the effort occurring at the federal level. State government officials across the United States have begun to understand that state governments can play a role in preventing cyber breaches, strengthening and updating state statutes, and shoring up cyber defenses to protect state and commercial assets and infrastructure.

Some state government cyber officials perceive the federal government as moving too slowly to enact new cyber policy. These officials are trying use state government mechanisms to act more swiftly to protect their citizens and businesses, as well as state government agencies. The purpose of this volume is both to describe progress being made by two states—California and Washington State—through highlighting each state's unique opportunities and challenges and to characterize the roles that nongovernment institutions play in influencing state-level cyber policy.

Qualitative interviews with state government officials provided the key inputs for the case studies presented below; additional information came from supplemental interviews and secondary document reviews. These case studies offer an initial look at the cyber policymaking environments in California and Washington State and the roles played by nongovernment organizations in those states. The results also provide some insights that may be broadly useful when seeking to understand cyber policymaking at the state level across the United States; however, these two case studies should not be used to develop conclusions about the nature of cyber policymaking at the state government level generally.

Centrally, the basic governance structure in each state, the relative strength of each branch or position, and resources available make a substantial difference in a state's ability to develop or consider types of policies, both generally and specific to cyber. State legislators' level of engagement can vary considerably in terms of the amount of time they spend on the job in different states: some legislators are full-time elected positions, while others are part time, and there is frequent turnover of legislators in many states. Legislative staff, who are assigned to legislators in some states, often lack relevant experience with or expertise in one or more policy areas; very few seem to have any experience on cyber issues.

The many state-level resource constraints often result in state legislators and their staff spending very little time on any specific policy initiative and having minimal if any substantive expertise to bring to bear on these issues. Compared with federal government legislators in Congress, state government legislators are much more resource constrained. Most of these differences are also evident when comparing state government agency officials and staff with individuals working at federal agencies.

1. Introduction

Although there are exceptions, in many or possibly most states, the cyber policy environment today appears to be particularly immature, and cyber issues are perceived as not very important, relative to other issues considered by state governments. In most states, when the legislature is considering multiple competing policy priorities, cyber policy receives little attention. Cultural differences and broad state interests also affect the types of cyber policy laws, regulations, and initiatives that may be considered and passed. Washington State, for example, is considered to have strong privacy laws based on cultural expectations of its citizens; in fact, multiple interviewees noted that its privacy laws are considered stronger than those that exist at the federal level.

States that have made cyber policy a priority often do so in response to a seminal event, such as a well-publicized, large-scale data breach. Both California and Washington State have had major data breaches in the past 5 years that have helped motivate state government officials to enact new cyber policy initiatives (described in more detail below), and other states such as South Carolina[1] and Utah[2] have also reacted to recent large data breaches by taking a more active role in cyber policymaking.

Our interviews suggest that the nature of cyber policymaking at the state government level varies widely among states, but all states are in need of additional resources (e.g., tools, frameworks, education, and training) to support more efficient and effective cyber policymaking. These resources need to be designed to support states with differences including structural and resource disparities, differing perceptions of how cyber policy is being or should be addressed at the federal government level, and cultural differences, among many others.

1.1 Study Methods

We chose two states as the focus of the case studies—for each state, the research team analyzed the cyber policy environment at the state level and the roles played by organizations outside of government. The state selections were based on anecdotal evidence suggesting significant cyber policy activity at the state level, coupled with a robust culture and reputation of high-tech industry. Table 2-1 summaries the interview participants. We conducted semistructured interviews with six individuals in California and nine individuals in Washington. Interviewees represented a wide range of agencies or departments: state legislature staff and elected officials; executive branch representatives in technology management, emergency management, and justice departments; and security intelligence sources. We conducted one additional interview with a professional association/consortium supporting state government agencies and two interviews with former federal government officials with expertise in this area.

RTI initially identified key agencies within the cyber policy communities in California and Washington State by consulting with subject matter experts and then leveraging contacts across existing networks to identify appropriate positions and individuals. Of 18 requests, 15 individuals accepted and participated in interviews, and three people either did not respond or were unable

Table 2.1 State Case Studies: Interview Sample Characteristics

	CALIFORNIA	WASHINGTON	OTHER
Core interviews	6	9	—
Current government officials	6	9	—
Informational interviews	—	—	3
Former government officials	—	—	2
Professional associations/consortia	—	—	1

[1] A 2012 data breach in South Carolina is described here: http://www.infoworld.com/article/2615754/cyber-crime/south-carolina-reveals-massive-data-breach-of-social-security-numbers--credit-cards.html.

[2] A 2013 data breach in Utah is described here: http://archive.sltrib.com/story.php?ref=/sltrib/news/56210404-78/security-breach-health-data.html.csp.

to coordinate their schedule to speak with us. Efforts were made to maintain a representative distribution of relevant cyber agencies within the interviewee sample and seek out top-level decision makers within each agency. Interviewees were informed of and asked to acknowledge confidentiality and anonymity protocols and had the right to refuse to answer any question or end the interview at any time. Interview content was not shared outside of RTI's internal team and Hewlett Foundation staff.

Interviews lasted approximately 1 hour and were conducted primarily in person, although several were conducted by phone. RTI researchers reviewed and cleaned the transcripts from each interview and subsequently conducted theme-based analysis of the transcripts.

As with the federal government interviews, in the questions posed to participants, the term "cyber" was intentionally left to individual interpretation. As a result, and in line with the Hewlett Foundation's definition of "cyber policy," "cyber" enjoys a broad interpretation for the purposes of this report. Qualitative findings from the study are aggregated and summarized below. We present responses thematically so that recurring themes in the analysis are highlighted. Although we make a few illustrative points, no responses should be interpreted as being representative of California or Washington State government, of any agency within these governments, or of any particular industry.

In addition to the case study interviews, we conducted secondary research for background purposes, focusing on recent cyber policy documents in the two states. This additional research helped us supplement and better characterize information collected during the interviews.

1.2 Study Limitations

The limitations of the case studies of California and Washington State echo the limitations mentioned for the federal government interviews, as described in Volume 1. In addition, many fewer individuals were targeted for interviews in California and Washington State than targeted for the federal government—the original objective of these case studies was to complete interviews with no more than five individuals in each state. Further, given the relative immaturity of cyber policy at the state level compared with the federal government, readers should use caution when interpreting and using the analysis results presented below. The cyber policy landscape in state governments appears to be changing very quickly, which could make the information presented below obsolete.

2.
Cyber Policy in California

2. Cyber Policy in California

Over the past 2 years, state government officials in California have become much more focused on cyber issues; critically, the state has been working hard to clarify roles and responsibilities and set a cyber policy strategy.

California is the home of some of the largest, most profitable companies in the world—including many of the largest technology companies and cybersecurity firms. Its economy represents 13.3% of the U.S. economy, and its population accounts for over 12% of the U.S. population. This combination of factors contributes to making the people and organizations in the state a very large and attractive target for cyber attacks. To prevent attacks from succeeding and to mitigate the results of cyber breaches affecting individuals and organizations in California, a combination of state, local, and federal government agencies and nongovernmental organizations have developed the existing cyber policy infrastructure.

Over the past couple of decades, the California state executive and legislative branches have issued multiple cyber-related laws, regulations, and guidelines with a focus on three primary objectives:

1. Creating protections for citizens' data with data breach reporting laws
2. Improving the cybersecurity of state agencies through procurements
3. Improving the cybersecurity of businesses through outreach/educational efforts

At the local level, several municipal governments in California cities—including San Diego and Los Angeles—have recently developed cyber-related initiatives, primarily aimed at educating citizens and local businesses about cyber risks and potential prevention and mitigation strategies. However, until very recently, clear roles, responsibilities, and leadership for cyber issues have been lacking in California. As such, the state has struggled to move beyond the objectives above and even to maintain focus on these areas. Both government officials and state legislators had been reluctant to jump into cyber policy debates.

Over the past 2 years, state government officials in California have become much more focused on cyber issues; critically, the state has been working to clarify roles and responsibilities and set a cyber policy strategy. In 2015, Governor Jerry Brown became more involved in discussing and proposing ideas on cyber topics, and the legislature, which in the past was not interested in considering new cyber policy ideas presented by a small number of representatives, has recently held multiple cyber-related hearings and passed several new laws. The current focus in the state is on building a better structure with which to address cyber issues: identifying and clearly delineating roles and responsibilities of state agencies and other stakeholders, developing a clear strategy for the role of the state, and improving the technical capabilities (staff) and information technology (IT) infrastructure of California state agencies.

2.1 Clarifying Roles and Responsibilities

In 2013, after the Target breach was reported,[3] cyber policy started to become more of a priority in California within the legislative and executive branches of government, most notably resulting in the creation of a new California Task Force on Cybersecurity, created at the direction of Governor Brown and overseen by both the California Office of Emergency Management (Cal OES) and the California Department of Technology. This task force—which includes individuals from the private sector, state government, federal government, academia, and law enforcement—meets once a quarter and has worked to identify ways in which the state can take on a larger role in cyber policy development. According to our interviews, this task force leveraged concerns following the Target breach[4] and the 2014 Sony breach to help build the base of support needed for cyber policymaking to gain some traction in California.

In August 2015, Governor Brown issued an executive order creating a new California Cybersecurity Integration Center (Cal-CSIC), under Cal OES. The Cal-CSIC will "…

[3] See more about the Target breach reported in 2013 here: https://oag.ca.gov/consumers/target-breach-information.
[4] See more about the Sony breach reported in 2014 here: http://fortune.com/sony-hack-part-1/.
[5] See the Governor's Executive Order here: https://www.gov.ca.gov/news.php?id=19082.
[6] See the Governor's Executive Order here: https://www.gov.ca.gov/news.php?id=19082.

2. Cyber Policy in California

serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions, and non-governmental organizations."[5] In addition, Cal-CSIC has been charged with developing "… a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices."[6] As of June 2016, the Cal-CSIC was still being formed—staff were being hired and policies and procedures written; as envisioned, it promises much-needed leadership and coordination for the state.

In addition to the establishment of Cal-CSIC, a February 2016 hearing on cybersecurity spending and activities in the state legislature shook things up further in California state government. The hearing highlighted the many state agencies that the state auditor found were out of compliance with state cybersecurity standards. During the hearing, the state Chief Information Officer and Chief Information Security Officer were both unaware of how much money was being spent on cybersecurity and could not comment on the lack of compliance with cyber-related regulations by state agencies or plans for addressing the situation; both resigned from their positions shortly after the hearing.

While California state government officials work to solidify state cyber policy roles, the National Guard is and has been playing an important role at the state level, and it could do much more. Based on national and state laws, the state cannot use the military for domestic issues; however, states can leverage the U.S. military resources through the National Guard. For example, as part of the U.S. military, the National Guard can access information on new threats, potential responses, and mitigation strategies and then use that knowledge to advise states without directly sharing classified information. The National Guard would like to increase its cybersecurity capabilities and has a good base structure to do so but lacks resources. Currently, state agencies are not required to conduct risk assessments of their IT systems, but ongoing discussions with the Governor's office and legislature may make this a requirement.

The state is also considering a variety of other cyber policy legislation,[7] including a "bug bounty" bill that would enable the state to

[7] See other draft CA legislation pending for consideration here: https://oag.ca.gov/privacy/privacy-legislation/leg (Note: This list, last accessed by the authors on September 1, is updated frequently so the number of cybersecurity bills pending will change).

California State Government: Key Roles

Legislative Branch. **The California State Legislature—including the Senate and Assembly—are responsible for designing, drafting, and passing new laws/regulations and budget authorization for state agencies.**

Executive Branch. **The Office of the Governor is charged with the execution of state laws and regulations, which involves developing policy initiatives and guidance as appropriate and needed. Within the executive branch, which is managed by the governor, the following are the lead agencies for cyber policy:**

- ***Office of Emergency Services (Cal OES)*** **—Manages all cyber incident reporting and response. Within Cal OES is the newly created California Cybersecurity Integration Center (Cal-CSIC), envisioned by the governor as the new lead for cybersecurity in California, including the creation and management of a state cybersecurity strategy and establishment of a Cyber Incident Response Team to "serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state."**
- ***California Department of Technology*** **—Oversees the security of all state government agency IT systems. Within the agency, the Office of Information Security plays a key role: managing and coordinating all state government IT system security measures, including ensuring compliance with all federal and state standards and law.**
- ***California Department of Justice*** **—Enforces all existing laws and coordinates with the U.S. DOJ. Recently and for the first time, the California Department of Justice issued guidance on unclear legal requirements for cybersecurity prevention measures.**

2. Cyber Policy in California

Interviewees suggested that many California lawmakers and other state officials did not sufficiently understand the technical factors at play when considering cyber issues, making it difficult for them to understand the potential risks to stakeholders in the state or to develop or assess the potential benefits of various solutions proposed.

pay citizens to find cyber vulnerabilities in state government systems. According to one participant, "The idea is to keep everything cost focused, use private markets. We developed this bill from talking to the tech world—Google and others. We asked what the state could do [to improve cybersecurity], and they suggested the state stand up a bug bounty program. California is the first state that will consider a bug bounty bill." Legislation such as this demonstrates California's willingness to innovate in its approach to cyber policymaking.

In the past and still today, many of California's state agencies' cyber responsibilities overlap significantly, and the state has no clear "lead agency" for cyber. The three agencies that have played the largest cyber roles in the state are Cal OES, the California Department of Technology, and the California Department of Justice. An overview of the roles played by these key agencies is provided in the text box above (see page 51).

Separately, but very importantly, the California state legislature and the Office of the Governor have played critical roles in establishing new laws and developing new guidelines and policies for implementation, respectively. The state legislature, which in past years was reticent to consider new cyber laws or even spend much time discussing cyber topics, has become much more active, holding hearings on cyber topics and passing several new laws (see a list of key cyber laws, guidelines, and initiatives passed or released in California in Table 2-2). As described above, the Governor has been quite active, issuing several executive orders which seek to better design the roles that the state will play to address cyber threats, and the Attorney General's Office (AGO) has gotten more involved in cyber policy, issuing guidance to companies on the cybersecurity measures they should have in place in order to comply with state laws.

A variety of federal agencies support cyber policy initiatives in California, including 6 Fusion Centers, part of a network of 78 national Fusion Centers funded by the Department of Homeland Security (DHS) but run by the states. Many of these, including the Northern California Regional Intelligence Center in San Francisco, have recently started to play a role in cyber information sharing by coordinating information sharing among local law enforcement; the private sector; and a variety of local, state, and federal government agencies. DHS also provides support to state agencies in California through the National Cybersecurity Communications Integration Center (NCCIC) and the Multi-State Information Sharing Analysis Center (MS-ISAC).

The U.S. Department of Justice (DOJ) also provides resources that support the state of California. U.S. DOJ shares information and resources with California DOJ to support prosecution efforts; U.S. DOJ also oversees the Silicon Valley Regional Computer Forensics Laboratory[8], which several California state government agencies mentioned as being very helpful in providing technical information on threats and other insights.

2.2 Understanding Cyber Policy in California

On many issues of public interest, California is often consulted for guidance on where the federal government and other states will be heading in the future. Many environmental, health, and safety regulations passed and implemented in California are later adapted by other states and the federal government.[9] In the case of cybersecurity, California was the first state to pass a data breach notification law in 2003, after which many states and later the federal government passed data breach notification legislation. However, beyond this law, California has not played a strong leadership role for other states or the federal government to follow.

California's lack of clear roles and responsibilities for cyber oversight has caused several people interviewed for this study to state that California is providing a bad example of how states should implement cyber policy at the state level. As of the publication of this report, several other states—including Washington, Maryland, and Virginia—seem to be considered the leaders in cyber policy strategy at the state level.

When asked why California has not played a larger role in cyber policymaking until recently, interviewees suggested that many

[8] See information on the SVRCFL here: https://www.rcfl.gov/about.

[9] For example, see: http://www.newyorker.com/business/currency/what-california-can-teach-other-states-about-climate-change.

2. Cyber Policy in California

California lawmakers and other state officials did not sufficiently understand the technical factors at play when considering cyber issues, making it difficult for them to understand the potential risks to stakeholders in the state or to develop or assess the potential benefits of various solutions proposed. Until the Target and Sony breaches in 2013 and 2014, state legislators and officials seemed to be comfortable letting the federal government set cyber policy.

After these breaches, many individuals in the California government decided that state-level action was indeed needed. As such, much progress has taken place over the last 2 years. A variety of new laws that have been passed or are currently under consideration by the legislature and the Governor's Executive Order authorizing the creation of the new Cal-CSIC offer a path for California to develop a strong, clear strategy for cyber policy in the state.

Table 2-2. Key Cyber-Related Legislation and Guidelines in California

NAME	EFFECTIVE DATE/ RELEASE DATE	BRIEF DESCRIPTION/PURPOSE
California Security Breach Information Act (S.B. 1386[10])	July 1, 2003 (original law)	**Requires organizations to notify California residents when their personal data have been stolen.** Enactment of a requirement to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
Revised California Civil Code Section 1798.81.5[11] (per A.B. 1710)[12]	September 20, 2014	**Mandates organizational security requirements.** Requires organizations to implement "reasonable security procedures and practices … to protect personal information from unauthorized, access, destruction, use, modification, or disclosure."
California Executive Order B-34-15[13]	August 31, 2015	**Directs CA state agencies, primarily OES, to take a number of actions aimed at improving coordination of cyber information sharing and proactive and reactive security strategy and implementation efforts.** Directs OES to create the California Cybersecurity Integration Center (Cal-CSIC), "which will be responsible for strengthening the state's cybersecurity strategy and improving inter-agency, cross-sector coordination to reduce the likelihood and severity of cyber-attacks." The Executive Order stated that Cal-CSIC will lead cyber threat detection, reporting, and response for the state.
California Electronic Communications Privacy Act (CalECPA), (S.B. 178[14])	October 8, 2015	**Requires state law enforcement to get a warrant before accessing certain types of electronic information.** Requires state law enforcement to get a warrant before they can access electronic information about who people are, where people go, who people know, and what people do.
California Attorney General's 2016 Data Breach Report[15]	February 16, 2016	**Provides clarification and guidance to organizations reviewing security requirements under existing law.** Sets forth the California attorney general's expectations on what "reasonable security" means, which indicates how the attorney general plans to interpret this phrase in Civil Code Section 1798.81.5.

[10] http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.
[11] http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5.
[12] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710.
[13] https://www.gov.ca.gov/news.php?id=19082.
[14] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178.
[15] https://oag.ca.gov/breachreport2016.

3.
Cyber Policy in Washington State

3. Cyber Policy in Washington State

Cyber policy in Washington State appears to be focused on educating citizens, business, and legislators on the importance of regularly updating IT systems and, for legislators, motivating the need to update cyber laws and technical policies and procedures to address the dynamic threat environment.

Washington State is considered by many to be a leader in advancing cyber policy for prevention, incident response, and technology. Our research suggests that the state government in Washington has been very deliberate in coordinating a number of interested parties in the state over the past 5 to 7 years to increase its cyber policymaking capacity. Cyber policy in Washington State appears to be focused on educating citizens, business, and legislators on the importance of regularly updating IT systems and, for legislators, motivating the need to update cyber laws and technical policies and procedures to address the dynamic threat environment. The state also seems to be very effective in engaging with federal partners and coordinating state agencies.

Many recent developments have focused on formalizing roles and duties for cybersecurity and protections in Washington State. Although its functions had been around for several years, in 2015, the Office of Cybersecurity was formally created within Washington Technology Solutions (WaTech), the state agency that manages state IT needs. In that same year, Washington initiated a partnership with DHS to reinforce the protection of state critical infrastructure and to create the new position of Chief Privacy Officer in the Washington State Office of the Chief Information Officer (which sits within WaTech). This new position is responsible for examining and providing input and guidance on privacy policies across state agencies, with a focus on strengthening protections for personal data.

In January 2016, Governor Jay Inslee signed an Executive Order (SHB 2875)[17] establishing a new state Office of Privacy and Data Protection within the Office of Cybersecurity. This new office aims to provide privacy training for and best practices sharing among state agencies and educate citizens about cyber threats. The legislation also further strengthened the Office of Cybersecurity, signaling the growing importance of cyber policy in Washington State. According to interview participants, the Washington State Office of Privacy and Data Protection is unique among states in its advisory role to the governor and legislature and also in the role it plays in raising awareness about privacy-related issues during the legislative process. In early 2016, the State of Washington hosted the inaugural Governor's Summit on Cybersecurity and Privacy,[18] where an audience of public- and private-sector executives and policy leaders was convened. This event provided a forum to discuss the latest cybersecurity and privacy issues, threats, and responses, as well as catalyzed conversation on how to gain efficiencies in deploying resources to ensure the state's economic resiliency and infrastructure security given the current cyber environment.

The government cyber policy community in Washington State also includes several other state agencies that contribute in various ways—the Washington Utilities and Transportation Commission, Washington State Department of Commerce, and Washington State Military Department's Emergency Management Division. These agencies work together with WaTech, the governor's office, and the state legislature to plan, coordinate, and unify the entire community to protect against and respond to cyber events.

Washington State has also worked to coordinate emergency response and prevention. Led by the Office of Cybersecurity, the state has taken a proactive response to train first responders and developers, to plan for a growing cyber workforce through educational initiatives, and to design technology with security in mind. State government officials have tried to emulate key federal government structures in designing the state systems; specific federal institutions that were mentioned include the following: MS-ISAC, NCCIC, the U.S. Computer Emergency Readiness Team (US-CERT), DHS, and the National Guard. Washington has also taken steps to establish its own

[17] See the legislation here: http://app.leg.wa.gov/billinfo/summary.aspx?bill=2875&year=2015.

[18] For more information on this event, visit: http://www.govtech.com/events/Governors-Summit-on-Cybersecurity-and-Privacy.html

[19] See the document here: https://www.snopud.com/Site/Content/Documents/cyber/Cybersecurity_WA_915.pdf.

3. Cyber Policy in Washington State

set of expectations for incident response and prevention within its state government system, even publishing its "Cybersecurity Guide for Critical Infrastructure for the State of Washington,"[19] which aims to delineate, address, and institutionalize cybersecurity in a manner that makes it an everyday priority for industry, educational organizations, and citizens. The guide aims to provide effective standards of practice, using the National Institute of Standards and Technology Framework as a guide to explain implementation strategies.

Washington State is also working with the federal government on educational tools that benefit states more broadly. For example, in 2016, Washington Governor Jay Inslee announced a pilot project with DHS and the MS-ISAC to create a playbook of critical infrastructure defense strategies that states and local governments can adopt.[20] This resource is expected to include information about cyber defense measures for government services, vulnerability identification and prioritization, and operational response and mitigation tools.

Discussions with key stakeholders in Washington largely confirm the sentiment that the state has been aggressive in recent years with respect to considering new cyber policies, passing laws, and implementing policies (see Table 2-3 for a list of recent cybersecurity legislation). Multiple participants described how the state has been crafting and updating its criminal law and internal state IT security policies over the past 2 to 3 years, as well as developing and maintaining relationships with local technology industry stakeholders and organizing interagency cooperation. A recent example of state cyber policy activity is the Washington Cyber Crime Act (2016),[21] a bipartisan bill that recognizes new categories of cybercrime that are not currently covered under law. This cybercrime bill updated the Revised Code of Washington (RCW) to make it more applicable to current data breach threats, such as tampering, spoofing, and distributed denial of services attacks.

Before adopting the Washington Cyber Crime Act, state prosecutors had been applying a statute defining and criminalizing theft to prosecute data breach crimes under state law. However, applying this statute became problematic because theft, as defined in the RCW, involves depriving the owner of the use of property; copying and subsequently distributing/selling copied data had not been contemplated. Updated RCW language corrected this oversight. As one participant explained the antiquated statutes, "Old legislation is geared to 'old school' hacking." The decision to update these statues required scrutinizing cybersecurity policies, examining legal precedents, and understanding and re-envisioning law enforcement's abilities.

[20] For background, refer to: http://www.governor.wa.gov/news-media/inslee-announces-measures-strengthen-cyber-security-and-digital-privacy

[21] See the legislation here: http://app.leg.wa.gov/billinfo/summary.aspx?bill=2375&year=2015.

Table 2-3. Recent Cyber-Related Legislation in Washington State

NAME	EFFECTIVE DATE	BRIEF DESCRIPTION/PURPOSE
ESHB 1078 (Consumer financial information)	July 24, 2015	**Strengthens data breach notification requirements to better safeguard personal information, prevent identity theft, and ensure that the attorney general receives notification when breaches occur so that appropriate action can be taken to protect consumers.** Provides consumers, whose personal information has been jeopardized because of a data breach, with the information needed to secure financial accounts and make the necessary reports in a timely manner to minimize harm from identity theft.
2SHB 1469 (Sensitive data/state network)	2015–2016*	**Prohibits state agencies from holding cardholder data or other payment credentials on state data systems.** Requires state agencies that currently hold payment credentials to work with the Office of the Chief Information Officer to eliminate the data from state data systems.
SHB 1470 (Cybersecurity panel)	2015–2016*	**Requires the Office of the Chief Information Officer to convene a blue-ribbon panel on cybersecurity.** Requires the panel to address (1) protecting critical infrastructure from the threat of cyberattack, (2) enhancing the security of the state's intergovernmental network, and (3) using best practices for local government response in the event of a debilitating cybersecurity incident.
HB 1561 (Information technology security)	2015–2016*	**Allows for consideration of IT security to be discussed in special sessions or meetings, if appropriate.** Requires the panel to address (1) protecting critical infrastructure from the threat of cyberattack, (2) enhancing the security of the state's intergovernmental network, and (3) using best practices for local government response in the event of a debilitating cybersecurity incident.
E2SHB 2375 (Cybercrime)	June 9, 2016	**Establishes the Washington Cybercrime Act.** Addresses the crimes of computer trespass, electronic data service interference, spoofing, electronic data tampering, and electronic data theft.
SHB 2875 (Office of data privacy)	June 9, 2016	**Creates the Office of Data Privacy, Protection, and Access Equity in the Department of Enterprise Services.** Allows the department to (1) serve as a central point of contact for state agencies on policy matters involving data privacy and data protection and (2) as a forum for ensuring equitable consumer access to communications and data technology. Requires the joint legislative audit and review committee to conduct a program and fiscal review of the office.
2SHB 1391 E2SSB 5315 (Aligning Consolidated Technology Services, Chief Information Officer, Office of Finance Management, Department of Enterprise Services)	2015–2016* October 29, 2015	**Transfers powers, duties, and functions of the Office of the Chief Information Officer within the Office of Financial Management.** **Transfers powers, duties, and functions of the Department of Enterprise services, pertaining to statewide IT services and applications, to the Consolidated Technology Services Agency.** Creates the consolidated technology services revolving account, the statewide IT system development revolving account, the statewide IT system maintenance and operations revolving account, and the shared IT system revolving account.
ESSB 6528 (Cybersecurity Jobs Act)	June 9, 2016	**Establishes the Cybersecurity Jobs Act.** Requires the Office of the State Chief Information Officer to (1) implement a process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines adopted by the State Chief Information Officer; (2) develop plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of public agencies in the event of a security incident; and (3) work with the Department of Commerce and other economic development stakeholders to facilitate the development of the state as a national leader in cybersecurity.

*= By resolution, reintroduced and retained in its present status, in the 2016 First Special Session.

3. Cyber Policy in Washington State

Washington has seen an influx of policymakers with experience in the technology industry over the past decade, adding technical understanding and interest in cybersecurity issues to the state legislature.

3.1 Understanding Cyber in Washington State

When asked to explain why cyber policy has been prioritized in Washington, interview participants offered several possibilities. First, Washington has seen an influx of policymakers with experience in the technology industry over the past decade, adding technical understanding and interest in cybersecurity issues to the state legislature. Washington State also recognizes the higher stakes associated with maintaining the cybersecurity of organizations operating in the state, given the high-interest targets located there, including several major technology firms (e.g., Microsoft, Amazon, Nintendo) and large military institutions (e.g., Joint Base Lewis-McChord). State officials have also noted an unexpectedly high volume of cyber attacks aimed at Washington State government institutions recently. Interview participants surmised that malicious foreign actors, perhaps unfamiliar with U.S. geography, were confusing Washington State with federal government institutions in "the other Washington" (i.e., Washington, DC).

Other, more indirect, drivers of cyber policy progress in Washington include the state government's desire to limit the state's liability and conserve scarce taxpayer dollars. "We talk a lot about exposure [and vulnerability]. A data breach should be the worst $300-400 million we spend." Washington would rather spend its scarce resources to educate and protect citizens, businesses, and critical infrastructure, rather than having to clean up after a cyber attack. Participants recognized that breaches could be measured not only by financial loss, but also by political fallout (e.g., failure to be reelected) and a general decrease in public trust of government. As mentioned earlier, recent data breaches targeting state entities both in Utah and South Carolina, where the jobs of some individuals in state government were threatened and the ability of state governments to protect its citizen's data was questioned, were cited as examples of what Washington seeks to avoid.

Notably absent from much of the recent cyber policy work in Washington has been the Attorney General's Office (AGO). According to interview participants, the AGO was the initial catalyst for a 2015 Breach Notification Bill, but otherwise has largely been silent (i.e., has not taken a position) on subsequent issues related to cyber policy, which surprised several individuals interviewed for this report. While no one interviewed could explain the AGO's lack of involvement, two individuals suggested that the AGO's priorities were simply on other forms of consumer protection.[22] In other states, such as California, attorneys general and Departments of Justice are supporting public education about cyber and actively work to enforce cyber policy laws through prosecutions.

[22] Note: RTI contacted the WA AGO for this study but was referred to other state agencies (especially WaTech) for interviews related to state cyber policy.

4.

The Role of Outsiders in State Policymaking

4. The Role of Outsiders in State Policymaking

Cyber policy stakeholders in both California and Washington State government look to federal government agencies as a model for government cyber policy development and implementation and for technical resources and tactical needs. Academics and other nongovernment organizations play a very minimal role in state government cyber policy development in either state, and our interviews suggest the same is true in many if not all U.S. states. California often looks outside of state government agencies for new cyber policy ideas, and it seeks input and feedback from nongovernmental organizations on ideas and draft legislation being considered. Based on our interviews there, California government policymakers and key stakeholders engage private-sector organizations, in particular companies that sell cybersecurity products or services, much more than any other group. Meanwhile, the view in Washington is that industry (especially defined as the technology industry) has been averse to being involved in staking any formal roles or positions in state cyber policy. Regardless, Washington has benefitted greatly from the experience of technology industry talent who have joined its elected ranks in the legislature.

When looking for information to inform cyber policymaking, state government officials usually look first to their trusted contacts and they search on the internet. In both California and Washington, key trusted contacts include government staff; in California, that core group also includes individuals working at private-sector security companies. In Washington, industry representatives may be consulted but infrequently and only informally. By far, the most consistent source of new information was simply talking to people and forming relationships. Human connections are considered to be the gold standard for information sharing in terms of receiving quality and relevant information (inefficiency notwithstanding). According to one state government official, "Personal connections are important because some of the information being exchanged, you definitely don't want shared with the wild."

Most individuals in both states mentioned receiving periodic digests of news clippings and industry research reports (e.g., Verizon's annual Data Breach Investigations Report). One participant reported skimming a technology journal monthly and several professional group magazines. Social media and blogs were infrequently cited as sources of information, while email listservs were more commonly used to keep up with topics of interest. Many individuals who were interviewed for this study expressed frustration that so few state-focused resources were available to them.

Washington State structured itself to have state counterparts to federal agencies to help create linkages and promote information sharing.

4.1 Federal Government

Cyber officials in the federal government often serve as resources to state government agencies, with individuals at DHS and U.S. DOJ likely engaging most often with state governments, including California and Washington State. DHS provides resources specifically developed for states; for example, DHS has developed information-sharing frameworks for states to use, and DHS provides funding for organizations like the Fusion Centers, which help coordinate local and state-level information sharing, including sharing information on cyber threats and solutions. U.S. DOJ supports state governments by sharing information when possible with state justice departments or attorney general's offices on trends and legal developments at the federal level.

Many states, such as Washington, also work to mimic the federal government structure to respond efficiently and effectively to any threat. Washington State structured itself to have state counterparts to federal agencies to help create linkages and promote information sharing.The complementary structure allowed for the development of a robust cyber emergency management structure with an actionable cyber breach response plan and provided both a structure and funding for adopting and managing effective cyber prevention.

States also look to various policies and initiatives coming out of the federal government. The White House and other federal executive branch agencies produce many useful documents, for example, the President's "Consumer Privacy Bill of Rights."[23] Reports such as this appear to have a substantial influence on many states' cyber policy strategies and priorities; in some cases, specific text from such reports ends up in state policy documents.

[23] See here: https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

4. The Role of Outsiders in State Policymaking

However, in most cases, federal cyber policy efforts and interests are very different from state government policy efforts and interests. Primarily, these differences are because the federal government manages most national security and foreign relations activities and has more resources, technical expertise, and efficiencies to tackle specific cyber issues and topics than states have. Given these differences, as well as the diversity of state government objectives, structures, and cultures, states seem to find it very difficult to use many federal government reports and legislation aimed at cyber issues.

4.2 Private Sector

In California, government officials noted that a variety of large private-sector companies, primarily in technology industries, regularly meet with members of the state legislature to provide input and feedback on cyber policy topics and potential legislation. Companies that sell cybersecurity products and services also meet frequently with various California state government agencies to provide technical expertise—offering insights into cyber threats and potential solutions—and, when appropriate, to market their products and services. As an example, one interview participant described convening a panel of academics, private industry stakeholders, and state government partners to discuss coordination of cybersecurity functions for the state. Reflecting on the discussion, this person noted that private-sector organizations provided the most useful information and suggestions, and this official specifically named the following companies: HP, IBM, Microsoft, Intel, and FireEye.

Our interviews from California suggest that technology and cybersecurity companies[24] play the largest role in providing input and feedback to the state government for many reasons. The following rationales were mentioned most often:

- Cybersecurity firms have technical expertise and are willing to provide targeted input and feedback on issues when requested.
- Technology industry representatives can comment from a firsthand perspective on the impact of new policies under consideration by their organization[25] (including the impact on jobs).
- Many of the cybersecurity firms that are asked for input and feedback are already working with the state government through product and/or service contracts.

In Washington State, interviews with government officials suggest that government engagement with industry is not as significant as in California. In Washington, several government officials noted that they do engage with private-sector individuals whom they trust, but in contrast to what we heard in California, private-sector industry in Washington appears to be hesitant to engage deeply with state government agencies or the state legislature on any formal level. Despite this difference in involvement, government officials recognize that industry approval is critical simply because industry owns so much of the critical infrastructure that is vulnerable to attack.

Industry in Washington State seems concerned that the public might react negatively if businesses were to become involved in certain types of policy debates, which may be related to the state's cultural tradition of protecting privacy and digital rights. For example, one interviewee stated that where proposed legislation brushes up against the digital rights community, the technology industry simply does not want to risk the potential negative publicity. When industry does take a stand on a cyber policy topic in Washington State, it grabs people's attention because it happens so infrequently. As one Washington legislator explained, "industry has been burned before," so it is wary to participate; as a result, in Washington State, the views of industry are more likely to be expressed privately than shared in a public forum.

4.3 Academics, Consortia, and Other Nonprofit Organizations

California cyber policy officials mentioned that they look to a broad mix of organizations and individuals in academia, research institutes, and other nonprofit organizations for input and feedback on cyber policy

[24] Note: Many technology companies, such as Apple, Google, and Microsoft, are not primarily cybersecurity companies; however, they do offer cybersecurity products and services. As such, the distinction between technology and cybersecurity companies is often very blurry.

[25] Several government officials in California stated that multiple companies have expressed concern about potential overregulation, noting that state regulation could be very costly if, for example, every state has a different cyber regulation with which companies operating in multiple states must comply.

4. The Role of Outsiders in State Policymaking

These organizations seem to offer a venue in which state government officials can get input and feedback on issues they are dealing with or hear about successes and failures in other states; such discussions can offer templates for new regulations or help stop a certain policy discussion.

topics; however, when asked specifically about the role that academics and other nonprofit organizations play at the state level, our interviewees suggested that such organizations play a very small role. Stanford University and the University of California at Berkeley were both mentioned during interviews, but no one we spoke with could name specific people whom they asked for information to help with cyber policy decisions. State government officials seem very interested in engaging with these communities more, but they noted that in the past when academics have been engaged, they have provided primarily theoretical ideas rather than practical or actionable information and recommendations.

In Washington, the role of academics varies widely depending on whom we spoke with in state government, but as in California, overall, academics seem to play a minimal role in cyber policy. The University of Washington (UW), Washington State University, and Stanford University were each mentioned once as being a group that might be consulted, although these institutions were named only after some probing. UW's Tech Policy Lab was cited by one participant as being helpful, although a different state government official described a situation in which the very same group at UW was invited to engage multiple times in state-level cyber policy discussions but never responded to the invitation.

In Washington State and in California, interview participants frequently mentioned several professional organizations that provide a mechanism for networking and information sharing. Organizations mentioned most frequently include the National Council on State Legislators, the National Governor's Association, the Council on State Governments, the National Association of State Chief Information Officers (NASCIO), and the National Fusion Center Association. Interacting with other advocacy and interest groups was minimal at the state level. These organizations seem to offer a venue in which state government officials can get input and feedback on issues they are dealing with or hear about successes and failures in other states; such discussions can offer templates for new regulations or help stop a certain policy discussion. Only one participant (from Washington State) mentioned having consulted or collaborated with the American Civil Liberties Union, Electronic Frontier Foundation (EFF), and Center for Democracy and Technology with regard to state-level cyber policy. Having the EFF to "officially take a neutral position" on proposed state cyber policy legislation (rather than outright oppose it, as had been expected and even feared) was considered a "huge win" by a Washington State legislator.

5. Challenges & Opportunities

5. Challenges & Opportunities

Cyber policy remains **predominantly a reactionary topic in most state governments**. As noted above, much of the recent cyber policy activity in both California and Washington State has been in response to high-profile data breaches. In Washington State, additional enabling factors include the election of several state legislators who understood the technical subtleties of cybersecurity and support from a variety of interest groups. In both states, a desire to avoid costly breaches has helped drive state government officials to form new positions and departments and to invest in new IT resources to minimize vulnerabilities and shore up cyber defenses.

Policies in both states have been described as more anecdote driven than data driven, which appears to be a function of both a general lack of data as it relates to cyber and an interest in the effect of policies (or lack thereof) on the personal lives of constituents. State legislators in both states noted that stories that can be related about the victims of an event, rather than a quantitative description of an event, often become the catalyst for action in their legislatures. The experience of victims can bring the issue home and make it relatable to others, especially to legislators who must be convinced to prioritize certain issues above others when they have many competing priorities.

Other aspects of cyber can make it difficult to sell to constituents and other policymakers. First, **it is difficult to demonstrate the success of funding prevention activities** (including cyber mitigation strategies). Calculating the volume and breadth of data breaches that were avoided by spending money on prevention or mitigation, especially doing it well, can be challenging. In addition, legislation on cyber issues in states such as Washington may find a split in terms of interest and prioritization between rural and urban areas. Legislators generally want to support policies on meaningful topics with observable results for their constituents. Constituents living in rural areas (where even internet connections may be spotty) are generally considered to be less affected by cyber issues than those living in urban areas. If a rural legislator's constituents are difficult to engage on the topic, it makes it more difficult to convince a state legislator that the issue deserves attention or support.

> One cyber official in Washington State stated that "many lawmakers don't know the difference between virtualization and mainframes"

5.1 Education & Training for State Officials

Almost all interview participants in California and Washington State noted that **uninformed policymakers and citizens present a central challenge to developing effective state cyber policy**. State policymakers' lack of understanding of cyber policy topics makes it very difficult to convince them cybersecurity is not simply a technology issue but also a public policy issue and that state government legislatures should prioritize it. Many lawmakers in both states do not seem to understand basic distinctions in technology (e.g., one cyber official in Washington State stated that "many lawmakers don't know the difference between virtualization and mainframes"). Moreover, they are intimidated by what they perceive to be cyber's complexity but also do not want to appear ignorant, so they do not want to admit what they do not understand. Meanwhile, cyber legislation does not have the same political dynamism as other political causes so that constituents rarely voice concerns or request action from their representatives. Finally, the results of cyber legislation, which are intended to be largely preventative, are not immediately or easily tangible and measurable, making it challenging for policymakers to convince peer legislators and constituents of the legislation's inherent value.

As an example of efforts made to improve cyber policy knowledge gaps, several interview participants in Washington State mentioned the Washington State Cybersecurity & Privacy Summit. Held in January 2016, this event was developed with the primary goal of meeting the need identified above: to educate and engage policymakers. Organized by the Washington State Office of the Governor and the Washington State Office of Cybersecurity, a division of WaTech, participants heard from representatives of the federal government, state executive branch, state legislature, digital privacy sector and those who own critical infrastructure. While heralded as a "win" in Washington State, some interview participants reported that it was not as well

[26] For more information, visit http://www.govtech.com/events/Governors-Summit-on-Cybersecurity-and-Privacy.html.

5. Challenges & Opportunities

attended by its intended audience (state legislators and staffers) as planners had originally hoped.

5.2 Workforce Development

Conflating the problem of inexperienced policymakers is the frequent turnover of elected officials. **High turnover rates in elected state government positions rarely allow for individuals to build connections, experience, or expertise beyond what they arrive with**. Related to this, interviews in Washington consistently mentioned a concern about a lack of skilled public-sector workers in the cyber environment. In California, all individuals interviewed noted that technical expertise is harder to obtain and keep at the state level than at the federal government level.

State governments need employees with a solid technical understanding of cybersecurity; at a minimum, they need help with technical and policy recommendations related to cybersecurity issues. Similar to what was mentioned in Volume 1 of this document, compensation packages at state and local government levels are not able to compete with what is being offered in industry.

Spotlight: State Intelligence Officers' Needs

Participants in intelligence roles have a different perspective and needs than those in the executive branch or legislature at the state level. First, the role of intelligence analysts is to anticipate potential events: to predict and project events based on the available information and intelligence. Second, these individuals are more likely to interact with individuals in cybersecurity (security intelligence) roles at local universities or think tanks rather than researchers.

What has been produced by the research and academic communities has very limited value for the intelligence community, and the most common concern is timeliness of the research results. Content is another concern, in that the intelligence community needs information that is immediately actionable. In a nonclassified environment, the findings of studies focusing on relevant cyber topics may be so "watered down" that they may no longer be useful.

Those in intelligence roles described their environment and proposed the following suggestions for the larger nongovernment cyber policy community to consider:

- **Many acknowledge there is "no good channel" for accessing information from think tanks and academics. The most commonly suggested venue was Google Scholar or networking connections. Indeed, conferences and networking opportunities are the best ways to reach intelligence analysts, for example, AGORA, InfraGard, and MS-ISAC (for specific threats). The only current research that state-level threat or intelligence analyst participants cited was the Pell Center Report.**
- **Useful topics of interest include identifying future threats or briefs focused on a specific technique or target. Conversely, papers focusing on the historical perspective on persistence of threat actors would not be useful.**
- **Would like to create internet-safe zones, akin to school safety zones. Small businesses can be hosted via web. Also, consider creating a safe space for seniors to be online, because they are frequently victims of fraud.**
- **While Washington State has open dialogue, there is a need to take it to the next level to better define roles and responsibilities, as well as resources and time. The state needs to further clarify state and federal roles and responsibilities because all cyber is linked and interconnected so that it is impossible to separate. Systems cannot be separated: emergency management, Homeland Security, and the CIO are focused on different aspects of what is essentially the same system.**

5. Challenges & Opportunities

As one official stated, "There are issues that are wonky for each state. We need more research and analysis that focuses on and account for the idiosyncrasies on the state level—how do states differ from one another and from the federal government in ways that may impact the ideal cyber policy strategy and specific activities for each state."

5.3 State-Specific Cyber Resources

Legislative and executive branch participants in California and Washington State noted that each had few examples from which they could build or borrow to craft language when forming state cyber policy. Although a few states were cited (Michigan and Virginia) as potential sources of information, the best source for ideas and guidance was federal legislation. However, as noted above, states find it very challenging to leverage federal government resources. Other respected sources included professional groups such as the National Association of State Legislators and NASCIO and, to a lesser degree, the National Governor's Association. Broadly, in both California and Washington State, government officials noted the dearth of state-focused cyber policy resources.

State structures and priorities are different from the federal government's structures and priorities. In California, several individuals noted the need for funding more state-focused research, analysis, and guidance. As one official stated, "There are issues that are wonky for each state. We need more research and analysis that focuses on and account for the idiosyncrasies on the state level—how do states differ from one another and from the federal government in ways that may impact the ideal cyber policy strategy and specific activities for each state." Although federal government stakeholders can use multiple resources on cyber policy topics, state government officials have far fewer resources. Similar to the federal government, state governments need help thinking about the potential costs, benefits, and other impacts of potential legislation. As an example, the state legislature in California had been considering developing robust information-sharing laws at the state level, similar to the CISA, which was passed at the national level. One interviewee said that since CISA passed, he has been considering questions such as: "Would a state information-sharing law like CISA have helped?" and "Would there been enough information shared to be useful or would it have been too costly, inefficient per organizations and for the state to manage?"

The state of California also needs a plan in place for incident response—including the role of the government and expectations of nongovernment organizations that are breached. Currently, state officials do not know who to contact for guidance. For example, after the Target breach that affected at least 70 million people was reported in 2013,[27] California did not have an incident response protocol in place, resulting in a slow response by Target and the state government. The state was not equipped to help manage the response or appropriately consider how the law should be altered afterward; however, per state law, state government officials were required to release data breach reports that included the Target breach.

After the Sony breach was reported in 2014,[28] a robust incident response plan for California had been instituted, and the response by state government agencies and Sony was much faster and smoother. Still, according to one interviewee, Cal OES believes that it has a plan in place, but many others do not feel it is adequately clear or comprehensive.

[27] See more about the Target breach reported in 2013 here: https://oag.ca.gov/consumers/target-breach-information.

[28] See more about the Sony breach reported in 2014 here: http://fortune.com/sony-hack-part-1/.

6. Conclusions and Recommendations

6. Conclusions and Recommendations

State cyber policy is very different from cyber policy at the federal level for many reasons. Therefore, state governments and other stakeholders need support and resources that are aimed at supporting the development and management of cyber policy at the state level, not at the national level. Compared with the federal government, states are more resource constrained (lacking the economies of scale to, for example, hire many technical experts on cyber topics), play more restricted oversight functions, and do not have a major role in either national security or international diplomacy issues, both of which are critical factors in cyber policy at the federal level. The lack of a geographic source for many cyber attacks adds to the complexity of state cyber policymaking.

As described above, broad differences in priorities and interests increase the disconnect between states and the federal government; further, states are very heterogeneous themselves. As state cyber policy initiatives mature, they will provide new examples and resources to other states, but a wide variety of resources and support are needed given the differences that exist in state policy environments.

Below are recommendations for stakeholders in the federal government, academia/nonprofits, foundations/philanthropies, and state governments. They represent a combination of RTI recommendations and recommendations offered by interview participants (the latter of which are noted). Many of the recommendations below could apply to more than one stakeholder group.

6.1 For the Hewlett Foundation and Other Funders

Foundations could play a critical role in helping fill the void of resources available to state government agencies working on cyber policy. State governments have insufficient budgets or are unwilling to support such research and analyses, and federal government resources are only helpful on some topics for state governments and on at a high level. One potential area of focus for foundations could be to fund cyber policy researchers to identify federal government resources that could be made useful for state governments and then to make the conversion. Depending on the number of resources that could be relatively easily converted, this effort could save money, as opposed to creating new resources from scratch.

State government officials in Washington requested the creation of new digests or journals that are more focused on cyber policy as opposed to being more technical in nature, as a way to help them identify relevant information. A publication such as this, with information specifically targeted at state governments, could act as a filter and help reduce the gap between technical and policy research. Several participants indicated that they would be eager to read such a publication, assuming it was correctly targeted at state government officials.

Broadly, foundations could support independent analysis of states' cyber policy environments to determine their relative strengths and weakness and to identity potential key causal factors. The resulting reports or briefs could help states identify ways in which they are succeeding, areas where they are falling short, and ideas for how to strengthen cyber policy in their states.

A final suggestion made by participants was to offer more objective didactic programming aimed at state legislators to help them understand cyber policy issues and reduce intimidation.

6.2 For Civil Society Organizations

As noted above, individuals interviewed in California and Washington State noted that academics have offered little support to state cyber policy efforts in the past probably because of a lack of interest by academics and their focus on more conceptual or theoretical topics. Although more conceptual and theoretical research could certainly benefit states in the future, academics could better support state government officials' stated needs by focusing on topics of interest to state governments in the short term (e.g., laws and regulations the legislatures are considering).

Legislators and legislative staff in both states suggested that more applied research by academics and nonprofits could help them make better cyber policy decisions at the state level. They made several specific requests: one legislator asked for new research to analyze the costs associated with data breaches for victims, as well as remediation activities for the affected

[29] Of note, the Hewlett Foundation is funding the Taxpayers for Common Sense to create a national database of U.S. government spending on cybersecurity. This database may serve as a starting point for the database requested by individuals in both California and Washington State.

6. Conclusions and Recommendations

organizations and the political risks involved (e.g., could data breaches affect legislators' ability to get reelected). To assess the value of a new security policy, legislators need to know "how bad [costly] a certain event could be" in terms of dollars of loss, legacy loss, mitigation costs, decrease in political trust, the number of policies affected, and even the number of press conferences that may result. This research could include a detailed post-data breach analysis to help develop a list of best practices and potential impacts. Legislators do not have this information, nor do they know how to calculate it. Legislators need a better understanding of these kinds of impacts.

Additional research that would help support legislators in many states could include analysis of the potential impact of successful attacks on critical infrastructure, such as the power grid and water infrastructure, or on other state government assets, such as correctional facilities (e.g., resulting in the release of inmates). New research on topics such as these should focus on impacts like the potential costs to affected stakeholders, liability, and the anticipated political cost of action or inaction before or after the event.

6.3 For the U.S. Federal Government

The federal government could do a much better job of providing information on funding of cyber-related initiatives and of cyber policy resources. Based on our interviews, states could benefit greatly from the creation of a national database compiling the agencies and efforts related to cyber policy that the federal government and state governments are funding.[29] This database should include cyber policy initiatives at the federal government and state government levels, noting the specific funding mechanisms used in each case and key resources developed, and should clearly describe the purpose of each initiative and resource developed. This database could help states better understand the separation between federal and state government responsibilities related to cyber—seeing where the federal government puts its dollars also helps states immediately understand the federal government's policy priorities. The database could also help states identify federal government funding that may be available to them and resources they might find useful. Such a database could be paid for by the government or paid for by others, such as foundations, but in either case, the support of government officials would make the resulting resource much more valuable.

6.4 For State Governments

State governments could do a better job of requesting support from the nongovernment cyber policy community, foundations, and the federal government. Few resources are aimed at supporting state government policy development generally compared with the resources available to the federal government, but almost none are aimed at supporting state government cyber policymaking. If state governments made efforts to clearly ask for help, the broader community, including academics, nonprofit researchers and think tanks, foundations, and the federal government, would likely listen and try to help. In Volume 1, the recommendations for federal government stakeholders provide some guidance that may also be relevant to state government officials.

Our research also suggests several broad recommendations for state governments to help them improve their cyber policy ecosystems. State governments could work directly to improve their cyber policy structures and processes by looking to other states as examples. State governments cannot easily change their basic governance structure (to be more adaptive to the pace of cyber policy issues), nor can they easily amend the technical qualifications of who is being elected into state office (e.g., to add lack of understanding of cyber as a disqualifying factor). However, they can work to enhance legislators' understanding of cyber issues, which is particularly needed given the dynamic nature of threats. And they can work to ensure the limited staff available to assist legislators are adequately briefed on policy issues surrounding cyber work.[30] State governments can also work to structure themselves after complementary federal government institutions, enabling them to leverage research, strategy, and operations resources developed for the federal agency.

They should also do what they can internally to encourage collaboration across divisions and institutions to provide a comprehensive, coordinated statewide effort that addresses emergency response, deterrence, and prosecution. Both California and Washington State are working hard at this, but both recognize that much more can be done to promote collaboration among public and private entities.

[30] Of note, Washington State has provided such programming aimed at legislators, but its effort resulted in limited success. Thus, more work designing effective programming may require new research and analysis.

Appendix A: Agency Abbreviations

AT&L = Acquisition, Technology, and Logistics (within DOD)

CIA = Central Intelligence Agency

CIO = Chief Information Officer

DHS = Department of Homeland Security

DOD = Department of Defense

DOJ = Department of Justice

FBI = Federal Bureau of Investigation

FCC = Federal Communications Commission

FTC = Federal Trade Commission

HSARPA = Homeland Security Advanced Research Projects Agency (within DHS)

NAS = National Academies of Science

NIST = National Institute of Standards and Technology

NPPD = National Protection and Preparedness Division (within DHS)

NSA = National Security Administration

NSC = National Security Council

NSF = National Science Foundation

NTIA = National Telecommunication and Information Administration (within DOC)

ODNI = Office of the Director of National Intelligence

OMB = Office of Management and Budget

OSD = Office of the Secretary of Defense

OSTP = Office of Science and Technology Policy

SEC = Securities and Exchange Commission

USSS = United States Secret Service

Appendix B: Some Ideas for Future Research

Based on our interviews, federal government officials widely believe that nongovernment members of the cyber policy community are not paying enough attention to certain types of cyber policy research. During our interviews, we asked officials if they had any specific ideas or requests for future research to share with the cyber policy community. The following is a list of the ideas and requests that were offered:

- How do the laws of armed conflict apply to cyber?
- More legal analysis of the political environment, how it applies to internet standards or human rights.
- Timely analysis of censorship and surveillance.
- Data on effective computer crime, including costs, using rigorous methods (not a simple survey of 1,000 people that makes massive inferences).
- An explanation of how the government interacts with the private-sector companies who own the critical infrastructure.
- Place to publish for an audience of federal policymakers, for example, a digest of academic articles. It could be separated into various categories (multiple audiences).
- A better way to filter all the information and opinions that come in. Figure out how to decrease the "noise."
- Game theory applied to cyber events. If a nation-state is behind a major breach, how should we respond? What are the trade-offs?
- How do you set up a deterrent strategy to cyber breaches?
- Research on encryption is still needed. That issue is no longer as immediately critical as it was earlier, but work on privacy versus security with respect to encryption is still necessary.
- An international comparison of issues related to cyber across main nation-states.
- Strategies/thoughts on how to grow the cybersecurity workforce.