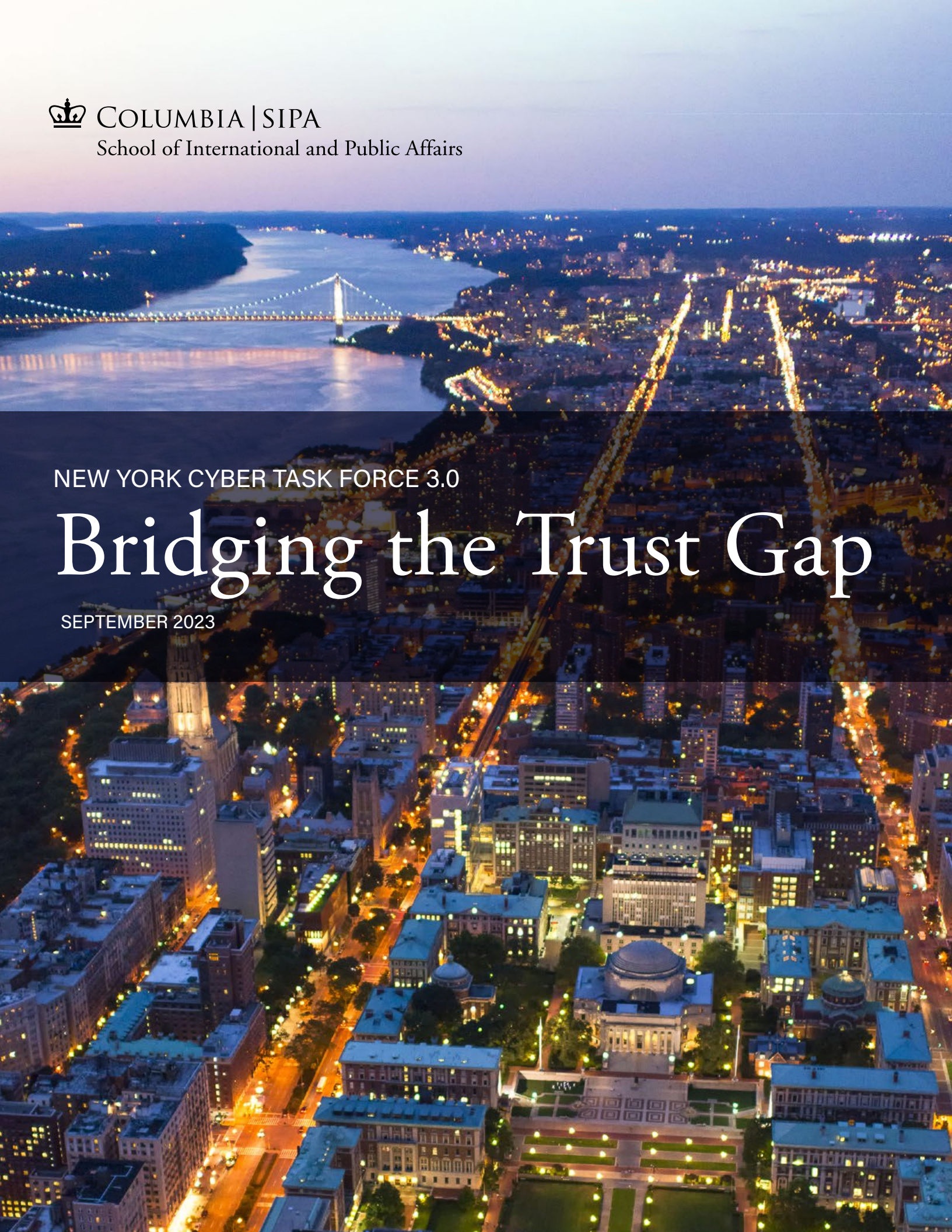

COLUMBIA | SIPA
School of International and Public Affairs

NEW YORK CYBER TASK FORCE 3.0

Bridging the Trust Gap

SEPTEMBER 2023

TABLE OF CONTENTS

FOREWORD

In this digital age, cybersecurity has emerged as a societal imperative. We have seen that when it falls short, privacy is shattered, businesses are put at risk, and national security is compromised. As the United States looks to meaningfully alter the public-private sector relationship through an ambitious National Cybersecurity Strategy, trust remains fundamental to a successful collaboration.

This third and latest report from the New York Cyber Task Force (NYCTF) drills down on the importance of trust in a cyber-secure future. The report captures the scale of the cyber threat, providing policymakers and industry leaders actionable and timely insights for how they can collaborate and foster trust to protect our digital landscape from malicious actors.

It is only fitting that the NYCTF is a product of Columbia University's School of International and Public Affairs (SIPA). Working out of New York City, the task force embodies a spirit of pragmatism and resilience, which is quintessentially New York and SIPA. There are few places that have the power to convene across sectors and to connect academic researchers with practitioners in the field to address real-world problems—in cybersecurity and every area we focus on at SIPA.

The NYCTF's first report from 2017 sought to give the greatest advantages to defenders over attackers at the least cost and greatest scale through the concept of leverage. Years later, that concept has been the guiding principle for the nation's National Cybersecurity Strategy. This report helps define new ways to strengthen the public-private partnership, and time will tell how its recommendations shape the policy landscape.

The scholar in me applauds its use of important case studies—including high-profile cyber incidents like SolarWinds, Colonial Pipeline, and Shields Up—to identify gaps and emphasize points of leverage to improve cooperation between the public and private sectors. The task force has captured the voices of experts and industry practitioners who are not only leading scholars of cybersecurity but also leading policymakers who have steered through some of the most notable cyber attacks of recent times.

I am proud that SIPA is the home of this task force. NYCTF provides the perfect example of how policy schools like SIPA can shape the public agenda and directly influence policy, whether in New York City or beyond.

Warmly,

Keren Yarhi-Milo

Dean, School of International and Public Affairs (SIPA)

Adlai E. Stevenson Professor of International Relations

Columbia University

New York, NY

MEMBERS OF THE NEW YORK CYBER TASK FORCE

Michael Bradshaw, Kyndryl
Chris Button, Analysis & Resilience Center for Systemic Risk
Beth Cartier, Maven Clinic
Byron Collie, J.P. Morgan Chase & Co.
Michael Daniel, Cyber Threat Alliance ◊
Scott DePasquale, Analysis & Resilience Center for Systemic Risk
Matt Devost, OODA
Amira Dhalla, Consumer Reports
Daniel Dobrygowski, World Economic Forum
Allie Friedman, Capital One
Misha Giridhar, Columbia University ∂
Nathanial Gleicher, Meta
Matt Goard, Morgan Stanley
Yasmin Green, Jigsaw
Jason Healey, Columbia University ◊
Niloo Howe, Energy Impact Partners
Merit Janow, Columbia University
Kristin Judge, Cybercrime Support Network
Elsa Kania, Center for New American Security
Elena Kvochko, SAP
Joshua Lane, Veeco
David Lashway, Sidley Austin LLP
Erica Lonergan, Columbia University †
Shawn Lonergan, PricewaterhouseCoopers
Peter Marta, Hogan Lovells
Ben Moskowitz, Consumer Reports
Jeff Moss, DEF CON and Black Hat
Craig Newmark, craig newmark philanthropies
Ian Pelekis, Next Peak
Erinmichelle Perri, Spotify
Neal Pollard, Ernst & Young
Shiva Rajgopal, Columbia University
Greg Rattray, Next Peak ◊
Blake Rhoades, Goldman Sachs
Monica Ruiz, Microsoft
Sal Stolfo, Columbia University
Leroy Terrelonge, Moody's
Phil Venables, Google Cloud
Daniel Wallance, McKinsey & Co.
Munish Walther-Puri, Presearch Strategy
Matthew Waxman, Columbia University
Evan Wolff, Crowell & Morning
Rebecca Wright, Barnard University
Pano Yannakogeorgos, New York University
Keren Yarhi-Milo, Columbia University ‡

† Executive Director
‡ Honorary Chair
◊ Cochairs
∂ Project Manager

ACKNOWLEDGMENTS

This report represents the consensus view of the members of the New York Cyber Task Force (NYCTF) in their personal capacity. We are grateful to the NYCTF members for their continuous support, participation, and contributions of expertise and knowledge to help develop insightful findings and actionable recommendations.

We would also like to thank the numerous individuals and organizations we interviewed as part of our research, who were extraordinarily generous with their time and expertise.

The New York Cyber Task Force is grateful for craig newmark philanthropies' generosity in making this project possible and thanks the Niejelow/Rodin family for their support.

EXECUTIVE SUMMARY

The New York Cyber Task Force (NYCTF) is a collaborative organization under the auspices of Columbia University's School of International and Public Affairs (SIPA) that brings together leading experts from academia, industry, and government agencies. The NYCTF's composition reflects its uniquely New York voice in the cybersecurity field. Its mission is to address cybersecurity challenges through research, education, and policy advocacy. The task force focuses on operational collaboration between the public and private sectors, conducting research to enhance cybersecurity practices, and providing guidance and recommendations to policymakers and organizations to make cyberspace more defensible.

The NYCTF has previously published two significant reports. The first, "Building a Defensible Cyberspace," was released in 2017. It provided recommendations aimed at strengthening the defense of cyberspace without compromising its utility and convenience. In 2021, the NYCTF released its second report, "Enhancing Readiness for National Cyber Defense through Operational Collaboration." This report presented a framework for operational collaboration based on a nodal model, using hypothetical future scenarios to identify ways of improving readiness.

This third report examines recent high-profile cyber incidents—SolarWinds, Colonial Pipeline, and Shields Up—to evaluate the private sector's perspective on operational collaboration. It uses these case studies to examine key gaps and identify points of leverage to improve how the government and industry work together. Over the past year, the NYCTF convened cybersecurity leaders and practitioners and conducted extensive interviews to investigate different perspectives on the case studies and the current and future state of operational collaboration. The task force report provides implementable policy recommendations to improve trust and operational collaboration between industry and government at scale. The report is organized around four key recommendations: improve US government crisis communications and transparency about cyber incidents; create professional incentives and opportunities for collaboration; establish a procedure for incorporating state and local stakeholders into operational collaboration; and establish a joint cyber warning center within the intelligence community.

Findings

The report identifies several key findings about operational collaboration that are common across all three cases, as well as those that are specific to the case studies.

In general, we found that:

- There has been significant progress in operational collaboration over the past decade.
- Challenges of trust in the government are enduring and multifaceted, lacking a whole-of-society approach. It is carefully cultivated over time, varies by context, and depends on grassroots, interpersonal, working relationships.
- The government faces challenges of effective crisis communication and coordination of messaging to the private sector.

- There is uncertainty within the private sector about how a growing regulatory footprint will affect operational collaboration.
- Effective operational collaboration often depends on size and maturity level, which is mismatched with the expectation that the government treats all companies equally.

Recommendations

The NYCTF report identifies four key recommendations, each buttressed by a number of supporting recommendations, to improve operational collaboration and trust. A core issue across the findings is that the US government typically has had three ways of interacting with the private sector: as a purchaser, regulator, or law enforcer. Yet none of these models is a good fit for operational collaboration. Therefore, our goal is to help define new ways of thinking about public-private collaboration beyond existing models.

Recommendation 1: Institutionalize crisis communications within the federal government. Multiple messages and communication channels from the government during an incident creates confusion and undermines credibility, trust, and effectiveness of response, especially when competing priorities are communicated.

Recommendation 2: Ensure that there are professional incentives and opportunities for collaboration within government and industry, and that the right people are in the room. People, expertise, and interpersonal relationships serve as the foundation for effective collaboration and the linchpin for cultivating trust.

Recommendation 3: Incorporate state and local stakeholders into operational collaboration. The federal government does not have the capacity to conduct incident response at scale for all state and local victims, and state and local governments vary significantly in cyber capability.

Recommendation 4: Establish a joint cyber warning center within the intelligence community that includes public and private sector elements. The warning should be clear about what the recipients of such information are expected or being asked to do as a response.

I. INTRODUCTION

Promoting a defensible and resilient cyberspace demands cooperation between the private entities that own and operate much of its infrastructure and the federal, state, and local government—in other words, it requires operational collaboration. Yet implementing effective collaboration remains an enduring challenge. Moreover, doing so rests on trust between the government and private sector, which can be difficult to establish and easy to undermine.

Collaboration remains essential because the cyber threat environment is dynamic and growing. Nation-state and criminal threat actors target industry and government with increasing scope, scale, and sophistication. In only the past three years, the United States has experienced a range of cyber incidents, from significant cyber espionage campaigns and breaches (such as SolarWinds[1] and Microsoft Hafnium[2]), to the identification of systemic vulnerabilities (such as the Log4j vulnerability[3]), to ransomware attacks against critical infrastructure with significant impacts (such as Colonial Pipeline,[4] JBS,[5] and Kaseya[6]). Moreover, since Russia's February 2022 invasion of Ukraine, the US and other Western nations continue to be on alert for the potential spillover of the conflict in cyberspace. Cyber incidents will also become increasingly public, at least for certain companies. This publicly will exacerbate the reputational costs that victims may face. It may also create potential regulatory and legal implications for certain industries, and it affects broader public perception of and confidence in both public and private actors.

Despite growing threats, there have also been notable successes. Over the past several years, there has been important progress with respect to operational collaboration. For example, in 2021 the White House released the Executive Order on Improving the Nation's Cybersecurity,[7] which, among other measures, aimed to reduce impediments to information-sharing, create a Cyber Safety Review Board (CSRB) to investigate cyber incidents, and improve software supply chain security, which could also have positive downstream effects on the overall cyber ecosystem. That same year, the federal government also established the Office of the National Cyber Director (ONCD), led by a Senate-confirmed National Cyber Director, to be a key touchpoint for engagement with the private sector; and elevated the role of cybersecurity within the National Security Council by creating a Deputy National Security Advisor for Cyber and Emerging Technology. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) established the Joint Cyber Defense Collaboration (JCDC) to be a locus of collaboration. This complements other collaboration hubs across the federal government, such as the Cybersecurity Collaboration Center within the National Security Agency (NSA).

The 2023 National Cybersecurity Strategy specifically adopts the ideas of leverage and operational collaboration as guiding principles.

Operational collaboration is a foundation of the Biden administration's 2023 National Cybersecurity Strategy.[8] In many ways, the strategy directly draws on ideas advanced by the New York Cyber Task Force (NYCTF). The NYCTF has long argued that the public and private sector should approach cyber defense and resilience using the concept of leverage, which gives the greatest advantage to defenders over attackers at the least cost and greatest scale, and via a robust program of operational collaboration. The 2023 National Cybersecurity Strategy specifically adopts the ideas of leverage and operational collaboration as guiding principles.

At the same time, the regulatory landscape has changed in a way that will inevitably affect how the government works with the private sector. In 2022 the president signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[9] which is creating new reporting requirements for the disclosure of information to CISA by covered entities. This legislation followed additional regulatory guidance promulgated for a number of critical infrastructure sectors, including new Transportation Security Administration (TSA) rules for the pipeline and transportation sectors. The Securities and Exchange Commission (SEC) has updated its rules to require publicly traded companies to disclose cyber incidents and other information. The 2023 National Cybersecurity Strategy makes an explicit call for the US to take more of a regulatory approach to cybersecurity and to hold certain actors liable for failing to remediate vulnerabilities. Altogether, these changes raise questions about what operational collaboration could and should look like in the future—one in which the relationship between the federal government and the private sector is evolving.

[This] NYCTF report reflects the task force's efforts to collect, organize, and reflect the private sector's experiences and expectations when working with the US government.

It is in this changing environment that the 2023 NYCTF, under the auspices of Columbia University's School of International and Public Affairs (SIPA), is weighing in on the state of public-private collaboration. Our objective is to provide meaningful and actionable policy recommendations to improve collaboration, building on existing progress. Specifically, the task force tackles three questions: How does the private sector actually perceive collaboration with the US government? What is the desired end state for industry with respect to optimal collaboration? What are the key policies and procedures necessary to bridge this gap?

To answer these questions, over the past year the NYCTF convened leading experts from business, policy, and academia to investigate the private sector's perspective on the current and future state of operational collaboration, as well as to understand the federal government's aims and aspirations in improving how industry and government work together.

The NYCTF's composition showcases its uniquely New York voice in the cybersecurity field. New York City is a hub for research and innovation with a culture and perspective that is distinct from other cyber centers across the country, such as Washington, D.C., or Silicon Valley. D.C. is often perceived as more "cautious" or "regulatory-minded" compared to the tech-forward optimism of Silicon Valley. While San Francisco and its surrounding areas embody the pioneering spirit of technological innovation, D.C. tends to approach technology with a more conservative and sometimes skeptical lens, prioritizing governance, oversight, and public interest. New York is the middle ground and balances these views to bring in a cautious optimism. In particular, our task force is practical and solution-oriented. We do not aim to provide a perspective on how the US government should be organized for cybersecurity issues or redraw the organizational chart that defines governmental roles and responsibilities for securing cyberspace. Instead, the NYCTF seeks to offer recommendations that can have the greatest leverage—identifying specific policy changes that are likely to have a broader impact on improving collaboration between the federal government and the private sector.

The 2023 NYCTF report reflects the task force's efforts to collect, organize, and reflect the private sector's experiences and expectations when working with the US government in the context of significant cyber incidents, as well as to identify potential gaps between how the government understands its efforts and how they have been interpreted by industry. The field lacks a systematic, empirically grounded assessment of the private sector's perception of how effective recent efforts at collaboration have been; the determinants of trust and credibility between stakeholders (a key element of effective collaboration); and the steps needed to improve these attributes. Grounded in extensive interviews with both private sector and government stakeholders about their perspectives on recent real-world case studies of collaboration—the 2020 SolarWinds breach, the 2021 Colonial Pipeline ransomware attack; and the 2022 Shields Up campaign—the NYCTF report provides a window into the state of operational collaboration. It also provides specific and tangible policy

recommendations to move the needle in a meaningful way to remedy gaps in collaboration to improve cybersecurity and resilience.

Background

The NYCTF published its first report, "Building a Defensible Cyberspace,"[10] in 2017. The report advanced a series of recommendations, anchored in the concept of leverage, to make it easier to defend cyberspace without sacrificing the utility, flexibility, and convenience that has made the Internet so essential to our economies and personal lives. This first report created a taxonomy of the defensive innovations that have created the greatest defensive advantage, at the largest scale, for the lowest cost. The task force found that some of the most effective defensive innovations have been organizational, rather than technical.

In 2021, the task force published a second report, "Enhancing Readiness for National Cyber Defense through Operational Collaboration."[11] This report adopted a future-oriented perspective, evaluating severe but plausible hypothetical future scenarios based on different drivers of cyber risk. The report offered findings on improving operational collaboration between the government and private sector based on a nodal model comprising networks of public and private stakeholders that could be activated across various contingencies. Additionally, an important finding of this report was the role of trust in enabling meaningful cooperation.

Objectives

The findings of the first two NYCTF reports, along with other, similar efforts, have contributed to a general consensus among both public and private stakeholders about the importance of operational collaboration to promote readiness and resilience. Indeed, in the past three years the US government has built and grown multiple mechanisms for collaboration with the private sector. This progress should be applauded.

At the same time, anecdotal evidence indicates that sentiment in the private sector about these efforts remains mixed. Lingering confusion about the implementation of operational collaboration and some concern about trust in the US government as a capable and credible partner contribute to this unease. While the government has attempted to articulate collaboration's value proposition to the private sector, in practice industry does not always perceive a clear upside. In some cases, collaboration may be seen as more of a burden than a benefit. Moreover, the changing regulatory environment is reshaping expectations in the private sector about what the future of operational collaboration will look like. Nevertheless, it is not necessarily the case that additional regulation will stifle collaboration. Indeed, the financial services sector is among both the most highly regulated critical infrastructure sectors—by state and local, federal, and international regulatory and supervisory bodies—and the most engaged in collaboration with federal government partners.

Therefore, our task force aims to evaluate and capture the true state of play of collaboration in practice across three recent case studies. We leverage the insights from the case studies to identify key findings for each case study, as well as findings that span across the cases. From these, we suggest implementable policy recommendations to improve trust and operational collaboration between industry and government at scale. Specifically, the report is anchored around four key recommendations: improve crisis communications about cyber incidents; create meaningful professional incentives and opportunities for operational collaboration within the public and private sectors; close the gap with state and local stakeholders; and institutionalize a joint public-private standing warning capability.

While the government has attempted to articulate collaboration's value proposition to the private sector, in practice industry does not always perceive a clear upside.

II. METHODOLOGY AND RESEARCH APPROACH

To evaluate the private sector's perspective on operational collaboration, our task force took a case study approach. We focus on two recent cyber incidents—SolarWinds and Colonial Pipeline— and the Shields Up warning campaign, each of which illustrate a different type of cyber threat as well as distinct challenges for public-private collaboration. At the same time, all three cases share similar themes.

Each case represents a different type of cyber incident– from a supply chain breach for nation-state espionage purposes (SolarWinds), to a cyber criminal ransomware attack against critical infrastructure (Colonial Pipeline), to an effort to provide early warning about anticipated malicious cyber activity before it might take place (Shields Up). Each one also reveals unique issues and challenges around operational collaboration.

We conducted extensive one-on-one interviews with a range of key stakeholders, focusing on leaders in the private sector, academia, cybersecurity experts, and nonprofits.

SolarWinds is a critical case because it was uncovered in December 2020 during a difficult presidential transition. As a result, the timing of the discovery set the tone for how the incoming Biden administration would evaluate and prioritize cybersecurity issues. Additionally, the SolarWinds case is unusual in that both the government and private sector were victims, potentially giving rise to tradeoffs on the government side between disclosing information and needing to protect government equities, especially around the nature, scope, and scale of the compromise. A private actor initially uncovered the incident and voluntarily reported it to the federal government, creating a situation where public-private collaboration was initiated by a private entity. Finally, the nature and scope of the incident—a sophisticated supply-chain breach that capitalized on a one-to-many scaling, compromising a wide range of targets—is a natural case for evaluating a key area where the government ostensibly has a comparative advantage in collaboration: being able to bring to the table a broader perspective across firms and sectors to understand systemic threats and vulnerabilities and communicate about them to wider audiences.

The Colonial Pipeline case represents an instance of a significant cyber incident targeting US critical infrastructure, but one that unfolded in a way that was not anticipated by many experts. In particular, while there have long been concerns about cyber attacks against critical infrastructure, many assumed that such an attack would take place at the direction of a nation-state actor. Instead, Colonial Pipeline was targeted by a criminal ransomware group, resulting in significant economic effects. Like SolarWinds, a private entity discovered this incident and reported it to the government. It also raises questions about gaps in the regulation of critical infrastructure; prior to the ransomware attack, the federal government exercised minimal cybersecurity regulatory oversight over the pipeline sector. Finally, this case stands out as an example of a significant government response, with law enforcement recovering a portion of Colonial Pipeline's ransom payment. Additionally, while not necessarily a direct result of the Colonial Pipeline, the US military has subsequently taken action to impose costs against and disrupt ransomware groups. This case also stands out as an example of a significant government response, with law enforcement recovering a portion of Colonial Pipeline's ransom payment. Additionally, while not necessarily a direct result of the Colonial Pipeline, the US military has subsequently taken action to impose costs against and disrupt ransomware groups.

Finally, the Shields Up case is distinct in that no significant cyber incident has taken place. Instead, Shields Up represents an example of an early warning campaign—an effort to share information with potential targets about

possible forthcoming malicious cyber activity resulting from Russia's February 2022 invasion of Ukraine. The Shields Up campaign, therefore, provides an opportunity to explore the government's attempts to get "left of boom" and collaborate with the private sector in anticipation of, rather than in response to, a significant cyber incident. This case also enables us to examine related organizations created to improve collaboration, such as the JCDC. While, as of this writing, Russia has not yet perpetrated major cyber attacks against the United States in the context of the Ukraine conflict, the potential cyber threat to critical infrastructure remains high. This provides us with an opportunity to explore both opportunities and challenges of long-term warning campaigns.

At the same time, SolarWinds, Colonial Pipeline, and Shields Up also share common themes: the private sector's trust in, and the credibility of, the government as a collaborative partner; issues of effective crisis communication and the utility the private sector perceives in information the government shares; common challenges around defining roles and responsibilities across various stakeholders; the extent to which there is clarity about how to engage the federal government; and how thresholds and scope conditions are defined, such as criteria for government involvement, definitions of critical infrastructure, and criteria for participation in different types of collaborative arrangements.

To evaluate these cases, as a first step we created a common case study framework. We began by examining open sources, including media and private sector reports, think-tank analytic products, and official government statements, reports, and testimony to identify important stakeholders, actions, and decisions for each case. We created a timeline of key events and mapped these to the statements, actions, and decisions of relevant public and private stakeholders. For example, we collected information about the initial discovery or identification of the incident, such as who discovered it, and the information that was communicated about the breach—how, to whom, and why. Furthermore, we explored how the government articulated its roles and responsibilities. We examined the classifications and triggers for thresholds and actions taken. Across all of these issue areas, we assessed what role, if any, the size, composition, or sector of firms played in determining their perceptions and responses.

As a next step, over the course of more than six months we conducted extensive one-on-one interviews with a range of key stakeholders, focusing on leaders in the private sector, academia, cybersecurity experts, and nonprofits. We also interviewed several current and former government officials, although our focus was on the private sector's perspective. In total, we engaged with nearly forty stakeholders. On the private sector side, the experts we interviewed were largely based in the financial services sector, big tech firms, cybersecurity firms, and the legal industry. While we acknowledge that this represents a limited subset of the US private sector, we deliberately chose to take a New York–based perspective, given the orientation of our task force.

We created a timeline of key events and mapped these to the statements, actions, and decisions of relevant public and private stakeholders.

Each of the stakeholders we interviewed was uniquely situated to provide an expert perspective on the case studies, and many were involved in the cyber incidents in some capacity. In Appendix 2 of this report, we have included sample interview questions for each case study.

Following the completion of the interview process, we held several internal task-force workshops to clarify and hone our findings, identify gaps, stress-test our analysis, and develop and organize our core and supporting recommendations.

III. CASE STUDY SUMMARIES

SolarWinds

In the midst of the presidential transition from the Trump to the Biden administration in December 2020, news emerged that a significant cyber incident had affected multiple US government agencies and private companies. The supply chain breach was traced back to a previously little-known firm, SolarWinds, a Texas-based software company that provides network monitoring and management software to many organizations. The malicious actors had gained access to SolarWinds' update server and inserted malicious code into the software update for the company's Orion platform. This code, known as SUNBURST or Solorigate, allowed the actors to access the networks of SolarWinds' customers who had installed the software update.[12] The code was disguised as a legitimate software update and went undetected for several months before it was discovered. Once installed on a network, the code communicated with a command-and-control server to receive instructions on data exfiltration.

> [SolarWinds] underscored the cybersecurity vulnerabilities of complex information and communications technologies supply chains.

The SolarWinds incident is distinguished by the scope and scale of the breach. It compromised tens of thousands of entities (although, ultimately, the threat actors exfiltrated data from a much smaller number of victims). The incident affected US government agencies, such as the Treasury Department, Department of Homeland Security, and the Department of Energy, as well as private companies like Microsoft, FireEye, and Cisco. It underscored the cybersecurity vulnerabilities of complex information and communications technologies supply chains.

While the US government did not attribute the breach to Russia's Foreign Intelligence Service (SVR), also known as APT29 or Cozy Bear, until April 2021, it was already apparent at the time of its discovery that the perpetrator was a nation-state actor.[13] As early as January 2021, a joint statement by the FBI, CISA, Office of the Director of National Intelligence (ODNI), and NSA described the incident as being "an intelligence gathering effort" carried out by an "Advanced Persistent Threat (APT) actor, likely Russian in origin."[14]

The US government was initially made aware of the breach by a private cybersecurity firm, FireEye/Mandiant, which discovered that its own networks had been breached and privately communicated information to the government as well as disclosing FireEye's compromise to the broader public.[15] The sophistication of the attacker's tradecraft, coupled with the theft of red team tools, is what prompted CEO Kevin Mandia to alert the government.[16] This alert triggered a scramble within the government to understand the scope and scale of the compromise across both the public and private sectors; assess the motivation of the threat actor, particularly whether the breach was part of an extensive cyber espionage campaign or was a prelude to a forthcoming disruptive attack; mitigate the damage and prevent further compromise; conduct attribution; and develop appropriate response options.

The Trump administration formed the Cyber Unified Coordination Group (UCG)[17] in December 2020 to coordinate the whole-of-government response, which the Biden administration stood down in April 2021. The government treated the SolarWinds breach as a national security concern, stemming from its wide scope, its links with the Russian government, and the burden placed on the private sector for incident response. Its response involved both immediate actions to contain the compromise and longer-term measures to prevent similar incidents from happening in the future.

The SolarWinds compromise is considered one of the most significant cyber incidents in recent history, with

far-reaching consequences.[18] The attackers were able to access sensitive government and corporate data, including intellectual property and personally identifiable information. The attack also exposed vulnerabilities in software supply chains and highlighted the need for increased security measures in this area. The incident has led to increased scrutiny of Russia's cyber activities and contributed to more strained diplomatic relations between the US and Russia. It has also resulted in a renewed focus on cybersecurity by governments, businesses, and the public. The full extent of the damage caused by the breach is still being assessed, and it is likely that the fallout from this incident will continue to be felt for years to come.

Colonial Pipeline

On May 7, 2021, Colonial Pipeline, a US company that manages an extensive pipeline system that delivers almost fifty percent of the gasoline and jet fuel along the East Coast, announced that it had decided to proactively shut down its pipeline operations after its information technology systems were hit with a ransomware attack.[19] Having gained access to Colonial Pipeline's information technology system through a compromised account on its virtual private network (VPN), the attackers encrypted its data and demanded a ransom payment in exchange for a decryption key. While the ransomware did not affect the company's industrial control systems that actually manage the pipelines, Colonial Pipeline indicated that its decision was driven by a precautionary concern about the hackers' potential next steps. The company also chose to make the ransom payment demanded by the attackers, which was 75 bitcoin (at the time approximately $4.4 million).

The ransomware attack and subsequent decision to shut down the pipelines triggered a domestic political and economic crisis for the Biden administration.[20] It generated alarm among the American public about fuel shortages, leading to panic buying and increasing gas prices. It also had spillover effects on other critical infrastructure sectors, especially the aviation sector, given its dependence on jet fuel, and it disrupted normal operations at a few airports as a result. Colonial Pipeline began to restore service six days after it had shut down the pipelines, although it took several days for the system to return to routine functioning.

Colonial Pipeline alerted the FBI that it was the victim of a ransomware attack, and the FBI was quick to publicly attribute the ransomware attack to the Russian-linked cyber criminal group, DarkSide, which was known for its ransomware-as-a-service model.[21] President Biden subsequently clarified that, while the attackers likely enjoyed safe haven in Russia, the US government did not believe the Russian government was directly responsible for the attack.[22]

The attack triggered a number of responses on the part of the federal government. Of note, CISA and the FBI published a joint advisory on May 11 containing information about the DarkSide ransomware-as-a-service variant to push information to the broader public.[23] The Department of Justice (DOJ) established a task force, the Ransomware and Digital Extortion Task Force, to investigate ransomware attacks. In June, the DOJ recovered about half of the ransom payment that Colonial Pipeline made to DarkSide, approximately $2.3 million, as a result of the FBI gaining access to the decryption key for the Bitcoin wallet housing the ransom payment.[24] In addition to imposing additional sanctions on Russia and announcing it had taken action to impose costs on ransomware groups, Biden officials issued direct warnings to their Russian counterparts about state responsibility for cyber attacks that emanate from within their borders, and in June 2021 President Biden met with President Putin in Geneva to warn Russia that sixteen critical infrastructure sectors were off limits for cyber attacks.[25] The Colonial Pipeline attack also contributed to the Biden administration's issuance of the Executive Order on Improving the Nation's Cybersecurity.[26]

Prior to the Colonial Pipeline ransomware attack, the federal government had imposed minimal cybersecurity requirements or standards upon the pipeline sector.

This incident underscored the vulnerability of critical infrastructure to cyber attacks and the significant variation across different critical infrastructure sectors in cybersecurity guidelines and regulations.[27] For instance, prior to the Colonial Pipeline ransomware attack, the federal government had imposed minimal cybersecurity

requirements or standards upon the pipeline sector.[28] In response to this incident, the TSA, which is the sector risk management agency for the pipeline sector, issued a series of three security directives.[29] The first directive was issued in May 2021 and included a mandatory reporting requirement of cybersecurity incidents within twelve hours of discovery. The second directive was issued in July 2021 (but was not made public until a year later) and was criticized by many in the industry for not reflecting an understanding of IT and OT systems in the pipeline sector. After incorporating industry feedback, a third directive was released in July 2022.[30]

Shields Up

Russia's February 2022 invasion of Ukraine prompted fears within the US government that Moscow would launch cyber attacks against US critical infrastructure in response to economic sanctions imposed against Russia or actions taken in support of Ukraine. Therefore, CISA launched its "Shields Up" campaign in early 2022 to serve as a form of warning about potential Russian cyber activity.[31] Around the same time, CISA's director, Jen Easterly, sent a letter to the members of the National Association of Corporate Directors, urging them to adopt a more vigilant posture and encouraging them to assess whether their organizations were implementing certain cybersecurity measures and practices.[32] She stated that cyber risk must be seen as a fundamental business risk, where ownership lies within the private sector as a matter of good governance.[33] Shields Up, therefore, is a use case of the government proactively warning of a threat that has not yet materialized—to get "left of boom."

The audience for Shields Up is wide in scope. It is aimed at organizations across all sectors, both public and private. The idea behind the campaign is to raise awareness about cyber threats; prompt organizations to implement heightened defensive postures in the context of an ongoing geopolitical crisis; and share information to other parts of the federal government, state and local governments, critical infrastructure owners and operators, the private sector, and the American public in general to improve defense and resilience.

Shields Up focuses on several key areas, including ransomware prevention, endpoint security, and incident response planning. Through Shields Up, CISA pushes out guidance about cybersecurity best practices; information about preparing for and responding to cyber incidents; and alerts and advisories about specific threat actors and malicious activity. The campaign also includes resources, such as webinars, tip sheets, and checklists, that organizations could use to assess their cybersecurity posture and implement best practices.[34] The campaign also emphasizes the importance of incident response planning and provides guidance on how to develop and test a robust incident response plan. Furthermore, Shields Up highlights the ongoing threat posed by ransomware and provides guidance about proactive steps organizations could take to prevent ransomware attacks from succeeding.[35] Additionally, the campaign underscores the need for ongoing investment in cybersecurity and the development of new technologies to stay ahead of evolving cyber threats.

Furthermore, in August 2021 at the annual Black Hat conference, Easterly announced the creation of a JCDC[36] within CISA. The stated purpose of JCDC is to be a hub within the federal government for operational collaboration, both across the interagency and with the private sector and state and local partners. For example, one element of the JCDC is a Slack channel established to enable real-time intelligence sharing. While the JCDC was established prior to CISA's Shields Up campaign, the JCDC has been an element of CISA's broader effort to be more proactive about potential cyber threats to the United States as a result of the Ukraine conflict. For example, the JCDC developed a plan for operational collaboration in the context of this geopolitical situation and conducted tabletop exercises, and the Slack channel has served as a complement to the public-facing Shields Up communications.

While there has not yet been a significant cyber incident targeting the US in the context of the Ukraine conflict, Shields Up remains an ongoing campaign.[37] Its ongoing nature makes it difficult to assess for effectiveness. Additionally, Shields Up has evolved beyond its initial objective of improving readiness and resilience in response to Russia's invasion of Ukraine toward a broader effort to raise the level of cybersecurity across the United States more generally. Easterly and then–National Cyber Director Chris Inglis, for instance, published an op-ed in June 2022 describing Shields Up as the "new normal" in cyberspace, while acknowledging the need for a sustainable approach to cybersecurity that avoids challenges of vigilance fatigue.[38]

IV. SUMMARY OF FINDINGS

Our research has generated several key findings about operational collaboration that are common across all three cases, as well as some that are unique to each incident. To evaluate these findings and their implications, we apply the framework developed by the first NYCTF report. That framework cataloged innovations in cyber defense over the past fifty years according to innovations in technology, operations, and policy. Rather than focusing on defensive innovations, we explore perceptions of gaps or challenges in collaboration that are largely about technology, operations, or policy. The below framework maps the findings to those categories.

Table 1: Framework of Findings

	Technology	Operations	Policy
Findings	**Finding 6.** The nature of the SolarWinds incident—its attack vector and scale—posed unique challenges.	**Finding 1.** There has been significant progress in operational collaboration over the past decade. **Finding 2.** Challenges of trust in the federal government are enduring and multifaceted, lacking a whole-of-society approach. **Finding 2.1.** Trust rests on informal, interpersonal relationships. **Finding 2.2.** There is a "say-do" gap that undermines trust. **Finding 2.3.** Differences in perceptions about the completeness of information- sharing affects trust. **Finding 2.4.** Overpromising and underperforming undermines trust. **Finding 2.5.** Trust issues within the government negatively affect private sector trust in government. **Finding 5.** Effective operational collaboration often depends on size and maturity level, which is mismatched with the expectation that the federal government treats all companies equally. **Finding 7.** The ways in which SolarWinds impacted the federal government affected collaboration and trust.	**Finding 3.** The federal government faces challenges of effective crisis communication and coordination of messaging to the private sector. **Finding 4.** There is uncertainty about how a growing regulatory footprint will affect operational collaboration. **Finding 8.** There was a lack of transparency on the part of the government about thresholds for responses in the Colonial Pipeline incident. **Finding 9.** Colonial Pipeline revealed a need for greater regulatory focus and guidance pertaining to cybersecurity and resilience—along with a need for expertise and capacity. **Finding 10.** Shields Up represents a potential-use case of early warning. **Finding 11.** The objectives of the Shields Up campaign lack clarity. **Finding 12.** Many questioned the utility of information being shared and noted ambiguity about who is the audience for Shields Up. **Finding 13.** Shields Up reveals the role of time and the challenges associated with long-term warning.

General Findings

As Table 1 illustrates, the vast majority of the findings about gaps in operational collaboration stem from challenges of operations and policy, rather than challenges of technology.

This conclusion suggests that even as the underlying technologies that enable improved cybersecurity and collaboration continue to mature and develop, technology alone is not sufficient to ensure robust and meaningful collaboration. Instead, collaboration depends on the human element: how individuals work together toward common goals in trust-based relationships.

It is also notable that a number of the findings below are not new. Indeed, they reflect issues and themes that cybersecurity experts have noted for decades. However, the fact that they continue to resonate as key challenges in operational collaboration only underscores the need to implement policies to remedy longstanding gaps.

Finally, these findings reflect industry's point of view, in line with the NYCTF's mission. While the task force did consult with some government personnel, the government's perspective is not fully represented. A government-focused perspective would likely identify gaps within the private sector.

Finding 1:

There has been significant progress in operational collaboration over the past decade.

There was remarkable consensus across our engagements that significant progress has occurred over the last decade in improving operational collaboration between the federal government and the private sector—even as many stakeholders identified ongoing gaps and areas for further improvement. Interviewees across sectors reported that the level of capability, understanding, and willingness by various elements of the federal government to engage with industry is much higher than it has been in the past. As one interviewee noted, "The fact that most companies take it as a given that they need to care about cybersecurity, and that senior government leaders also take it as a given, is significant progress in itself." Another remarked, "Many years ago, the conversation was that 'we should involve the private sector,' but they were involved after fact, if at all—now, the private sector is part of the process."

Some attributed this change to sheer necessity: cyberspace demands operational collaboration, and the dynamism and growth of the threat environment has forced industry and government to figure out how to work together. Others attributed it to a more deliberate shift in approach on the part of the government to be more proactive about incorporating industry. One example offered was the decision by the Biden administration to include representatives from the private sector in the Unified Coordination Group at the White House that was established in 2021 to address the Microsoft Exchange breach.[39]

Moreover, across the three cases we examined, many agreed that the government appears to be learning. SolarWinds largely manifested as an issue of trust; Colonial Pipeline was primarily a challenge of transparency; and Shields Up contained issues of unclear objectives and audiences. A maturation is taking place over time across the three cases, demonstrating that the federal government is learning and adapting at a relatively rapid pace.

At the same time, despite the consensus that collaboration has improved, across all three case studies most interviewees identified gaps and issues that have persisted for some time. Much of the sentiment about improved collaboration appears to reflect an assessment that the government is taking the concept seriously (or that it is using the term in the first place, in lieu of "information sharing"), but gaps in implementation remain, particularly with scaling solutions. Both SolarWinds and Colonial Pipeline reflect challenges of scaling—a finding that dovetails with the first NYCTF report's focus on innovations at scale.

Additionally, some elements of the government have matured their capabilities for collaboration more so than others, and this difference may account for the apparent tension in the findings.

Finding 2:

Challenges of trust in the federal government are enduring and multifaceted, lacking a whole-of-society approach.

A nearly universal consensus is that trust is not only essential for effective collaboration but is also elusive and easily undermined. Interviewees generally agreed that trust is difficult to define but it is deeply related to the credibility of one's interlocutor, which in turn rests on their

ability to follow through on commitments and the veracity of the information they provide. They described trust as being carefully cultivated over time, varying by context, and dependent on grassroots, interpersonal, working relationships. Given the fickleness of trust as a concept, it is not surprising that many interviewees saw a need for significant improvement in this area. Many examples of a trust gap stood out across our outreach efforts; we highlight a few of these below.

- **Finding 2.1:**
  Trust rests on informal, interpersonal relationships.

  One hallmark of trust is the extent to which organizations are willing to allow junior personnel to interact with one another through informal working groups or similar unofficial mechanisms. However, such interaction is necessarily in tension with the formalized institutions, structures, and bureaucracies established by both government and industry for collaboration. On the one hand, if trust is personality dependent, then developing mechanisms to institutionalize these relationships risks eroding those factors that facilitate trust in the first place; or, as one interviewee remarked, "If you formalize it, you kill it." On the other hand, depending on the vagaries of interpersonal relationships risks privileging those entities with better access and relationships over others; and it also gives rise to recurring cycles of trust building and rebuilding as personnel changes occur both in the government and industry. Attempts to standardize trust in digital systems to invent technical solutions may be necessary, but it is not a sufficient long-term solution.

  Relatedly, many noted that the interpersonal nature of trust is deeply related to the size of a collaborative group. Trust has been most effectively cultivated in smaller groups where all participants know one another. As the size of the group expands, it becomes more difficult to establish trust and participants are less willing to voluntarily share private information. Additionally, most agreed that trust must be cultivated in the steady state and that it cannot simply be conjured or manufactured during times of crisis. As one interviewee expressed it, "You do not want to be in a position where you are exchanging business cards at the site of a disaster." Furthermore, interviewees agreed that trust can easily be undermined by missteps. Some pointed to CISA's February 2022 letter to the National Association of Corporate Directors as setting a tone that undermined trust with industry, with one interviewee remarking that the letter came across as conveying that "industry hasn't done enough and now it's your time to step up." Finally, many pointed to the importance of in-person engagement to establish trust—something that has been challenging to reestablish coming out of the COVID-19 pandemic. As one described it, "You don't establish trust via alerts or advisories. It has to be more face to face and interpersonal." In the case of the SolarWinds incident, for example, many noted that interpersonal relationships played a significant role in communication and collaboration. Similarly, preexisting relationships played a role in the Colonial Pipeline incident.

- **Finding 2.2:**
  There is a "say-do" gap that undermines trust.

  One manifestation of challenges of trust came in the form of a "say-do gap"; or, in the words of one interviewee, the federal government "needs to secure its own networks before offering to help secure the private sector's." This gap was particularly salient in the context of the SolarWinds incident but was a common thread running throughout the other cases as well. With respect to SolarWinds, for example, the incident itself was seen as undermining industry's trust in the credibility of the government as an interlocutor, because it was the federal government itself that was ostensibly the primary victim of the breach—and that clearly struggled in the beginning weeks of the incident to understand the scale and scope of its own compromise. Yet some in industry felt that the government was "telling the private sector what to do when it didn't even understand the scope of its own breach."

  Additionally, some elements of the federal government were lacking in basic cybersecurity practices that are essential for incident response. And when it came to accountability after the fact, the "say-do gap" manifested in a different way. The 2021 CSRB was established via executive order in response to SolarWinds, and the first agenda item for the board was supposed to have been investigating the SolarWinds incident—in the words of the executive order: "The Board's initial review shall relate to the cyber activities that prompted the establishment of a UCG in December 2020."[40] Nevertheless, the CSRB's first report tackled the Log4j vulnerability, rather than SolarWinds,[41] without a clear explanation from federal officials.[42] This change left many of those we interviewed uncertain about whether the

government had conducted a full after-action report of SolarWinds and if lessons learned had been identified and addressed, which also contributed to undermining trust. One interviewee noted that it is still not clear whether the government is doing enough "in its own backyard to prevent another SolarWinds. And this undermines trust and credibility with industry."

Others pushed back on this view, noting that it is challenging to have perfect visibility within large corporate networks; therefore, it would be unreasonable to expect the federal government to be any different—particularly when the federal government is not a single entity but, instead, is a sprawling and diverse set of entities. Similarly, another interviewee remarked, "The intelligence community is not omnipresent, and there are limitations on where it can collect, and this creates blind spots that adversaries exploit."

- **Finding 2.3:**
  Differences in perceptions about the completeness of information-sharing affects trust.

Another trust gap stemmed from very different perspectives among industry and government interviewees about the completeness of the information the government is sharing with the private sector. Specifically, many in the private sector believe that there is additional information that the government could—and should—share with industry but it is choosing not to do so for various reasons (a common assumption was classification). Many emphasized that the government—given its ability to see across verticals and have a broader picture of the threat environment beyond a particular industry, coupled with its access to all source intelligence—should be able to provide timely context and prioritization to industry to help identify the signal through the noise of cyber threat intelligence information. As one interviewee noted, "The number of alerts, vulnerabilities, and problems that any large enterprise is trying to deal with on its network is pretty large and you need a good case for why you want to upend everything and get people to change their priorities."

Particularly for the more mature players in the private sector, they expressed that they have little utility for commodified threat information that they already receive from multiple sources, particularly from external cybersecurity vendors. One interviewee remarked that, "Collaboration is not information-sharing, but it is working through discrete issues and problems together to find a solution and resolve the matter through a series of processes with tools and techniques that can be shared between the collaborators." As another interviewee described it, "What we really need [from the government] is information that 'wows' me—that we could not get from a private sector entity." For instance, with respect to both the SolarWinds and Shields Up cases, many interviewees noted that they would have benefited from strategic threat intelligence from the government, or otherwise unreleased timely tactical information about threat actor activity upon which they could take immediate and specific action.

Many expressed frustration with the JCDC, noting that they were not receiving useful information from those feeds–which some attributed to not having the right people on the government side participating in the JCDC Slack channels. For instance, one interviewee remarked that "the government should put the 'Joint' into the Joint Cyber Defense Collaborative. It would be especially useful to have representatives from the intelligence community meaningfully participating in these efforts and sharing unique information and context with industry."

Yet, on the government side, a number of interviews dispelled what they described as a belief in the private sector that "the government is sitting on more knowledge than it really is, and if we would just share that last little bit, then everyone would understand and things would be better." As one noted, "To some degree, if your phone isn't ringing, you are probably okay," then elaborated: "The private sector often thinks the government is holding back specifics, but that is often not the case; or, the level of detail that the government provides would not actually be useful or would put at risk the government's ability to get that information."

- **Finding 2.4:**
  Overpromising and underperforming undermines trust.

Another source of trust issues was a sense that the federal government was often attempting to solve more problems than it was capable of, taking on additional missions and responsibilities before being effective at the ones it already had. As one interviewee remarked, "The government should stop trying to be like a Mandiant and instead lean on its areas of comparative advantage." Trust issues were compounded when

there was a perception that, at the same time that it was expanding the scope of its remit, the government was also underperforming in key areas, such as when information shared by the government was not timely or was inaccurate, or misattributed (or not appropriately attributed); or when the government was perceived as not being transparent.

For example, some noted that, in the context of the SolarWinds incident, a number of private-sector stakeholders believed that they were receiving the best information from anonymous leaks to the media about US government actions and assessments, rather than directly from the government. In another example, some pointed to the cybersecurity directives stemming from the Colonial Pipeline incident as undermining credibility—and, by extension, trust—because they appeared to be mismatched to the operational realities of certain sectors, particularly in the area of operational technology and industrial control systems. Others pointed to the Log4j vulnerability, noting that one element of that incident that undermined trust was the perception that CISA used the "bully pulpit" of the government to galvanize interest and attention across industry, but did not provide specific, useful information that would enable firms to rapidly identify the vulnerability. When this was followed by the use of the bully pulpit again for the Shields Up campaign, "industry is just exhausted by it, lacks trust in the government, and as a result these efforts are not motivating action."

However, this perceived mismatch between overpromising and underperforming did not universally apply across the federal government. Indeed, most interviewees emphasize that there is significant diversity on this issue, with some elements of the government being highly effective, credible, and capable collaborative partners. For example, many emphasized the successes of collaboration with the NSA (especially its collaboration with the defense industrial base), and law enforcement, as well as some sector risk-management agencies (SRMAs), such as the Treasury Department. In particular, variation in the maturity level of different SRMAs was identified as a critical issue affecting trust and, by extension, the effectiveness of collaboration. One interviewee commented that, "Much of the effectiveness of collaboration is contingent on the capacity and maturity of a sector's SRMA."

- **Finding 2.5:**
  Trust issues within the federal government negatively affect private-sector trust in government.

  Finally, another factor undermining trust is industry's perception that there are trust issues *within* the federal government, which in turn undercuts the trust industry has in government. A number of interviewees commented on the fact that the government often does not speak with one voice, an issue we will address in greater depth in the next finding. An interviewee noted, with respect to the SolarWinds incidents, that there were "challenges within the Executive Branch as well as on the Hill with respect to effective communication. This was a bigger problem than communication to the private sector. And it had spillover effects of eroding the credibility of the government and feeding the suspicion that the government is incompetent and can't even secure its own networks." Additionally, many mentioned that efforts to get multiple representatives from different government agencies in a room together—let alone on the same page—made things "go sideways."

Finding 3:

The federal government faces challenges of effective crisis communication and coordination of messaging to the private sector.

A significant frustration expressed by industry is that the federal government often does not speak with one voice. When asked about the most impactful recommendation our task force could make, one interviewee emphatically stated: "For the government to be able to speak in one voice, not fifteen." This was echoed by another interviewee, who noted that "the technology is the easy part. Communication is the hard part." Many interviewees noted that multiple messages and communication channels from different elements of the federal government during an incident creates confusion and undermines credibility, trust, and effectiveness of response—especially when competing priorities are communicated by different parts of the government, prompting industry to refocus crisis mitigation goals. Interviewees emphasized that there is significant value in government crisis communications—which is distinct from more tactical and operational forms of information-sharing about cyber threats and malicious activity. Indeed, crisis communications is one of the core competencies of government. Similarly, others noted that government crisis communication serves a range of important purposes, such as conducting attribution,

providing information and context during a crisis or contingency that enables cyber defenders to prioritize, and promoting transparency around government actions and decision-making. With respect to the Shields Up case, for instance, many commented that the government's crisis communications on the cusp of Russia's February 2022 invasion positively focused attention on cybersecurity issues at the highest levels of corporate leadership, empowering cyber defenders to secure greater resources and prioritization.

There was, however, a consistent perception that the government often fell short in the area of crisis communications across the cases we examined. For example, many remarked that in the context of the Colonial Pipeline incident the federal government could have been more transparent in communicating to industry about why this particular case prompted a significant government response—to include the recovery of the ransom payment—and, by extension, why most victims of similar types of ransomware attacks should not expect that level of support. With respect to the SolarWinds incident, many expressed frustration that the "ground truth" continued to change, and that industry did not find government communications around the incident to be credible because multiple, conflicting pieces of information were put out by different elements of the government. Ultimately, many companies relied on information from cybersecurity vendors, industry peers, nonprofit organizations, and sector-based information-sharing organizations.

However, this challenge is fundamental to the organization of the government itself. First, different agencies have different missions and priorities that are not always in concert. Further, Congress has deliberately made certain agencies independent from the President and the Executive Branch, such as the Federal Communications Commission or the SEC. As a result, as one interviewee noted, "There is no one in the White House who can tell the SEC that its incident reporting requirements are creating challenges with collaborating with the private sector on a particular cybersecurity issue or incident." In effect, the government's bureaucratic structure is set up for failure when interagency coordination is required. This structure exists for good reasons, but it creates unintended negative consequences in the realm of cybersecurity collaboration. Executive Branch coordination problems are compounded by congressional independence, which, while essential for democratic government, further hampers the ability of the federal government to speak with a single voice and contributes additional messaging confusion around cybersecurity incidents. One interviewee put it this way: "From an industry perspective, unless someone has spent years inside the US government and understands all of these distinctions, it can be frustrating and difficult to understand why the government can't seem to get its act together." This complexity raises questions about how reasonable it is to expect private sector players to understand the intricacies of how the government is structured and the implications for government communication. On the other hand, since we want to maintain the checks and balances necessary for a democratic government, these structures will not change. Enabling industry to understand government structure and how it affects messaging in broad terms while synchronizing communication within the Executive Branch seems like a reasonable compromise.

Relatedly, concerns about equity hang over many government interactions with the private sector. For instance, if an individual on the NSC staff meets with one company, they have to be willing to meet with any and all similarly situated companies in order to avoid the appearance of bias. As a result, the answer is often not to meet with anyone. Navigating these issues from the government side can create significant risk and downside, while the benefits are intangible.

Finding 4:

There is uncertainty about how a growing regulatory footprint will affect operational collaboration.

The federal government's approach to cybersecurity regulation has changed markedly over the past few years. While the 2023 National Cybersecurity Strategy most recently underscored this evolution, this theme ran throughout all three cyber incidents. The SolarWinds incident prompted the Biden administration to update cybersecurity requirements for the federal government; Colonial Pipeline revealed the patchwork nature of cybersecurity regulation of certain segments of critical infrastructure; and the Shields Up campaign kicked off around the same time that President Biden signed CIRCIA into law, creating reporting requirements by covered entities to report substantial cyber incidents to CISA. These trends prompted industry stakeholders to speculate about how a growing regulatory approach would change—if at all—the nature of operational collaboration. The crucial difference, many noted, between collaboration and regulation is that the former is voluntary, while the latter is compulsory.

Some expressed concerns that, with respect to CIRCIA for example, CISA taking on more regulatory-like functions is likely to have a dampening effect on collaboration. One noted that "companies share information with some government partners that they would not necessarily share with a regulator." Others were starker in their assessment of the implications of CIRCIA legislation, with one interviewee commenting that "the idea of working collaboratively is over." Others, however, acknowledged that the level of private sector investment in cybersecurity across the board is simply not high enough—with the exception of a few companies in highly mature and capable sectors. Therefore, the fact that the government is moving toward a regulatory regime with more baseline requirements is not surprising—and will also not vitiate the need for operational collaboration in areas where either the government or the private sector lack critical information or the ability to act. As one interviewee remarked, "Credit should be given to CISA for running a robust industry engagement process (at least so far) in the development of the incident reporting regulation. That's a good example of how to engage industry first before regulating."

Nevertheless, frustration with the apparent lack of coordination between different regulatory efforts was clear, despite messaging coming from the government that regulation would be harmonized. For instance, some pointed to the simultaneous efforts by the SEC and CISA to promulgate new requirements without apparent coordination. While most acknowledged that better visibility on the part of the government is an inherently good thing, it remains an open question as to how the government will use and share information that is reported to it by the private sector; whether the information being shared will actually enable the government to achieve desired outcomes; and whether the government has clearly defined those desired outcomes and communicated them to industry. Some observed that commentators often distort the industry's take on regulation: "It's not that having no regulation is a good thing, but there needs to be a more optimal balance. And the right set of people need to be involved in discussions about regulation—especially technical experts talking to each other."

However, regulatory agencies have a delicate balance to achieve. They have to take sufficient input from industry to make regulations feasible, but they cannot appear to be "captured" by the regulated industry. That tightrope is difficult to walk.

Moreover, those we engaged in government shared a different perspective. Many noted that the most regulated sectors, such as financial services and the defense industrial base, are also among the most collaborative. Most said that the idea behind increased regulation is to raise the lowest common denominator, rather than impose additional regulations on already highly regulated sectors. However, it is not clear that this message is being effectively received as such by industry, particularly given industry's reaction to the recent efforts at regulation of critical infrastructure, such as the TSA's initial security directives in the wake of the Colonial Pipeline incident.

Finding 5:

Effective operational collaboration often depends on size and maturity level, which is mismatched with the expectation that the government treats all companies equally.

Some pointed to a growing maturity on the part of the government in terms of shifting away from treating the private sector writ large as a single stakeholder toward taking a more sophisticated approach with respect to engaging different elements of industry for various types of challenges, and appreciating the range of capabilities, maturity, interests, vulnerabilities, and risks that reside across firms in the private sector. In turn, this evolution has engendered greater willingness on the part of industry to share information and collaborate with government partners who are seen as credible and understanding. Not everyone shared this view, however, and others were more skeptical, pointing in particular to CISA's approach as being "one size fits most." Paradoxically, a "one size fits most" approach ends up fitting very few entities in the private sector, resulting in an unintended outcome in which the more mature firms see less value in information being provided (and may even find it to be distracting or counterproductive), while the smaller and less capable firms—which ostensibly are in greater need of support from the government—lack the ability to usefully ingest the tools and information being offered. One interviewee stressed that the government should provide "more tailored information, based on an understanding of the specific audience, that is shared in a way that the sector or firm can actually digest. This may mean working differently and at a higher level with more mature players than with less mature ones. But this is fundamentally in tension with the current approach."

Overall, therefore, a key finding is that those entities with the maturity and resources to operationally collaborate with the federal government already have access to much of the information the government has as well—if not, in some cases, better information. In contrast, those that lack the resources, preestablished interpersonal relationships, organizational maturity, and know-how to engage with the government may be the greatest potential beneficiaries of collaboration, but these benefits have gone unrealized. Relatedly, one important gap concerns the role of state, local, territorial, and tribal actors (SLTT). Similar to private industry, SLTT entities face significant cybersecurity threats but vary in terms of their organizational maturity, size, skill, and capacity to engage with the federal government. Some of the more mature entities expressed frustration with the quality and depth of collaboration with the federal government and have commented that they receive better quality and more useful information from private cybersecurity vendors than from the government. One interviewee remarked that "we are still in a 'gangs of New York' situation where it's the private sector that state and local actors are going to rely on." Others expressed frustration at the lack of integration of SLTT entities into federal collaboration structures—especially those that are well positioned to ingest information from the federal government and act as credible and capable collaborative partners. At the same time, they pointed to the significant disparities across SLTT entities and the perception that the less mature players are not receiving sufficient support or able to engage the federal government. Thus, while the National Cybersecurity Strategy, for instance, emphasizes in multiple places the importance of federal government collaboration with SLTT entities, such collaboration has not yet been meaningfully implemented and that integrating SLTT entities into federal government operational collaboration efforts should be accelerated.

Case-Specific Findings

Additionally, we identified several findings that were specific to each case study. They are detailed below.

SolarWinds Findings

Finding 6:

The nature of the incident—its attack vector and scale—posed unique challenges.

Several critical aspects of the SolarWinds incident challenged policymakers in ways that impacted operational collaboration. The nature of the breach—targeting the information and communications technology supply chain—resulted in an impact that was significant in terms of scope, scale, and range of targets (both public and private). This crystallized a perception within the federal government that SolarWinds posed an urgent threat that demanded an effective and rapid response. SolarWinds prompted the federal government to look inward to examine its own cybersecurity practices. It also raised questions about the implications for other widely used IT products from a macro cybersecurity perspective. As one interviewee noted, this incident spoke to challenges of trust in the cybersecurity supply chain: "The SolarWinds incident had downstream effects on end users that implicitly rely on the trust of third-party providers that whatever they are providing is secure." Another noted the counterintuitive effects of the incident, noting how "the clients that we normally are on top of for poor patch management approaches in this case were not affected by SolarWinds; and it was those who were more effective in their timeliness of updating software who were victimized."

For the federal government, the one-to-many scaling of the SolarWinds incident strained its ability to understand the scope of the compromise and to respond in a timely and effective way. Yet the scale of this type of incident should have been an area where the federal government would naturally excel, given the government's visibility across silos.

One interviewee reflected how SolarWinds changed how experts conceptualized public-private collaboration and incident response: "We thought about significant cyber incidents as one entity being affected, and the Federal government and other elements of the private sector rally around that victim. But when large-scale breaches take place, the government lacks a way of evaluating where and how these incidents manifest risk to critical infrastructure across sectors and articulating the role of the government in terms of incident response." Moreover, the fact that the breach was uncovered during a presidential transition added to the challenges of the government's response.

Finding 7:

The ways in which SolarWinds impacted the federal government affected collaboration and trust.

SolarWinds was also unique in that it affected both the federal government and private industry. Many

interviewees noted that it is precisely these kinds of cross-sector, systemic cyber incidents that should be an area where the federal government has an advantage in visibility and assessing the scope of the compromise. In theory, the federal government should be able to see across verticals and have a more complete and cohesive understanding of the threat environment and the breadth of cyber incidents, while individual entities can only observe threat actor behavior on their own networks coupled with information they may receive from industry groups and cybersecurity vendors. But, in practice, SolarWinds demonstrated that the government lacked that visibility. Indeed, one of the most significant barriers to effective collaboration at the outset of the incident stemmed from the federal government's inability to rapidly assess the impact of the breach.

Some of this inability was due to internal challenges within the government itself. Some departments and agencies, for instance, were self-reporting compromises, while others were not. Additionally, some elements of the federal government initially erroneously maintained that they were not breached due to poor cybersecurity practices. For instance, one interviewee observed that one of the government departments their firm worked with simply did not retain logs that went sufficiently far back in time and, as a result, assumed they were not breached because they lacked the data. Overall, as another interviewee noted, this "revealed that there was no common policy across the whole of government about what information should be reported, to whom, and under what conditions." In other words, different parts of the federal government had different practices and protocols. As a result, the government "was ineffective in understanding how it needed to potentially reallocate resources to respond because it has an incomplete view of the impact across the ecosystem." A secondary effect, this structure hindered credibility and trust in the government by the private sector. This decrease in trust was further compounded by the fact that the government was not the first to identify and disclose the breach.

Additionally, the fact that the federal government was itself a victim of the breach—indeed, the primary victim—created unique tradeoffs in the government's decision-making about how to respond and what information to disclose. One interviewee reflected that SolarWinds "highlighted gaps in response and communication protocols when the US government is both itself the target and trying to respond to victims in the private sector." Being a victim hampered incident response when the government was sensitive about the extent of its own compromise.

That said, many companies are reluctant to reveal details about breaches and incidents while they are ongoing. Therefore, it would be unrealistic to expect the federal government not to have some concerns about revealing the extent of the SolarWinds breach. That incident was clearly the work of the Russian government, which created concerns and caution on the part of the US government. Also, given the access that the Orion software provides, when the breach was initially uncovered it was not a foregone conclusion that the operation was purely espionage. It could have been for disruptive purposes and revealing too much about what the US government knew could have prompted Russian action.

Colonial Pipeline Findings

Finding 8:

There was a lack of transparency on the part of the government about thresholds for responses.

The Colonial Pipeline ransomware attack prompted a significant response on the part of the federal government, and included action taken by the FBI to recover the ransom payment. The timeliness and significance of the government's response was viewed by many as a positive step forward, and many noted that there was effective collaboration across the government and the private sector, especially between the FBI and private sector partners in the legal industry.

At the same time, some expressed concern about the lack of transparency about criteria and thresholds for government action as well as lack of communication on what was already being worked on. While no one expects the government to disclose sensitive decision-making or other information that would undermine operational security, more general transparency would be helpful.

Most assumed that the federal government chose a more aggressive response due to the perceived impact of the ransomware attack on the economy—despite the relatively small ransom sum demanded by the attackers and the fact that the company decided to take the pipeline offline as a proactive measure, rather than due to an actual attack on those systems. But the lack of clear communication about responses created some confusion and undermined trust.

For example, it prompted other victims of ransomware to question why they had not received similar levels of government intervention, especially for larger ransom payments. One interviewee said that the week the Colonial Pipeline incident took place, they "received calls from multiple clients asking about when they would receive their funds back. The level of involvement by the government in the case of Colonial Pipeline confused some people and probably mis-set expectations."

On a related note, others remarked that the government's decision in this case to not form a UCG to coordinate the federal government's response to the incident, while it had done so for the Microsoft Exchange breach and SolarWinds, raised questions about consistent and clear thresholds for informing government responses. Others noted that the Colonial Pipeline case raises broader questions about how the federal government is tackling ransomware, particularly given the emphasis in the National Cybersecurity Strategy on conducting more assertive disruptive campaigns against ransomware actors. Many observed that the government lacks "transparent criteria about the role of the military versus law enforcement in 'imposing costs' against ransomware groups."

Finding 9:

Colonial Pipeline revealed a need for greater regulatory focus and guidance pertaining to cybersecurity and resilience—along with a need for expertise and capacity.

The Colonial Pipeline ransomware attack revealed the need for greater regulatory focus and guidance pertaining to cybersecurity and resilience of critical infrastructure. In particular, it underscored the significant heterogeneity across critical infrastructure sectors in terms of level of cybersecurity regulation (if at all) and the maturity and capacity of SRMAs to engage with their respective sectors. One interviewee stressed that the pipeline sector "was an industry that was largely unregulated, and Colonial Pipeline made it clear that the government had to be seen as doing something." At the same time, the incident revealed a need for greater expertise within the federal government around critical infrastructure, especially OT environments.

Following the Colonial Pipeline attack, federal, state, and private entities took extensive measures to fortify the oil, gas, and electric infrastructure against persistent vulnerabilities. A government reaction to the Colonial Pipeline attack was the Strengthening American Cybersecurity Act (SACA) passed the following year.[43] It required federal agencies and critical infrastructure owners and operators to report cyber attacks within seventy-two hours and ransomware payments within twenty-four hours. A week after the Colonial Pipeline attack, President Biden issued an executive order, initially drafted following the SolarWinds incident.[44] Executive Order 14,028 focused on enhancing supply-chain security, fostering better information sharing between the government and private sector, instituting a Cyber Safety Review Board, and formulating a comprehensive strategy for addressing cybersecurity weaknesses and events.[45]

However, many interviewees expressed frustration with the government's reticence to involve the affected sector in drafting the cybersecurity regulations, which they noted has broader implications for how industry is likely to perceive forthcoming guidelines and requirements. There was a perception that there was a lack of sufficient industry input. One interviewee lamented that "there is a tendency to regulate industry first, and then consider feedback from industry second." And as another elaborated, "Following the Colonial Pipeline ransomware incident, there was a rush by TSA to promulgate several security directives—but the later security directives essentially unwound the problems created by the earlier ones."

For example, the later security directives lengthened the initial timeline for incident reporting and changed the vulnerability management and patching cadence.[46] In particular, initially there was a requirement that systems had to be updated whenever patches were pushed;[47] but many interviewees noted that, in industrial control systems environments, pulling systems offline to patch and update will cause interruptions in essential services, such that artificial deadlines could have the unintended consequence of disrupting operations.

One concern that many highlighted was the fact that the first security directive was not made public; instead, "the companies in that industry that were subject to it were sent confidential letters spelling out the details. This caused initial confusion in terms of what pipeline companies would be required to do and how the security directive was coordinated with existing regulation." Another interviewee reflected that, "If the government had just sought out industry input to begin with, there would have been better security directives at the outset." Others underscored how some of the initial guidance that the federal government

promulgated was inconsistent with best practices. In particular, one interviewee stressed that "the TSA and broader federal government's approach to leveraging unique authorities to fill perceived gaps in cybersecurity standards is going to run afoul of where industry has largely achieved some consensus, such as ISO, NIST, or other international standards."

While this incident contributed to political consensus around breach notification and disclosure about ransom payments, there continues to be a lack of clarity about what the government will do with cyber incident information and how such information will be shared within the federal government. As one interviewee put it, "It puts a big burden on companies and organizations to share private information without a clear understanding of its purpose and use."

Shields Up Findings

Finding 10:

Shields Up represents a potential use case of early warning.

The Shields Up campaign was set up in light of Russia's impending attack on Ukraine. The geopolitical landscape, therefore, prompted a first-of-its-kind warning campaign to raise awareness about the importance of securing systems against cyber threats and take proactive steps to mitigate risks posed by cyber attacks. While it started as an "imminent" warning, it subsequently evolved over time into a steady state. In this sense, many interviewees remarked that the Shields Up campaign serves as a potential-use case of what government warning could look like. They also noted some of its early successes. Government communication about the Russian threat was useful in that it galvanized firms into action and reinforced the significance of cyber threats to senior corporate leaders. It also provided a vehicle for the federal government to reinforce messaging around basic cybersecurity measures, such as multifactor authentication, and provided basic guidelines for securing systems against ransomware attacks.

Finding 11:

The objectives of the Shields Up campaign lack clarity.

Despite its potential utility as a form of early warning, many raised concerns about a lack of clarity around the objectives of the Shields Up campaign. The information provided has been more descriptive and educational than focused, streamlined, or prescriptive. Some wondered if the government has effectively defined what it meant to be "Shields Up"—in other words, to clarify what Shields Up looks like and means in practice. In the words of one interviewee, "Shields Up is no longer motivating and lacks specific actionable steps that can be institutionalized." Others noted that it is not clear whether the goal of the campaign is to improve overall cyber defense and resilience or to put firms on a higher alert posture for a defined period of time in anticipation of an acute cyber threat.

Additionally, many observed that the campaign primarily focuses on prevention measures, such as endpoint security and ransomware prevention, rather than detection and response measures. These distinctions are significant because they suggest different types of actions and investments that private-sector actors should take. For instance, while prevention is important, organizations should also have robust monitoring and detection capabilities to identify and respond to cyber threats in a timely manner. One interviewee remarked, "It's not clear what action the government wants firms to take in response to Shields Up. Specifically, it is not clear what the criteria and behavior are beyond basic cyber hygiene practices. For example, when do SOCs need to go on heightened alert status? When should they implement compensating controls?" Relatedly, some underscored the need to differentiate between Shields Up as a broad concept that covers many aspects of basic cybersecurity and the specific elevated defensive posture in response to the threat stemming from Russia's invasion of Ukraine. In other words, "Shields Up has taken on a life of its own, and it's no longer clear what specific purpose it is serving."

Finding 12:

Many questioned the utility of information being shared and noted ambiguity about who the audience for Shields Up is.

A near-universal consensus from our outreach is that the private sector perceives significant issues with the usefulness of information being shared as part of the Shields Up campaign, and this has corroded perceptions of the effectiveness and utility of some elements of the federal government as a collaborative partner. One interviewee described Shields Up as sharing "yesterday's news"; information often lacks timeliness, novelty, or lack utility for the more mature players in the private sector—further underscoring the discrepancy between the utility of information for large versus small firms. They emphasized

that Shields Up would benefit from sharing both more strategic intelligence and granular context, as well as having greater clarity about the specific audience, objectives, and required actions. However, it is worth noting that information *is* being shared, and this sharing represents an important improvement.

Many highlighted that the intelligence community (IC) should play a critical role in making a campaign like Shields Up effective, but noted that, in their experience, the IC is playing a negligible role in this effort. Others noted that the private sector should be involved in shields Up as a source of useful information *for* the government, not simply as a consumer of information pushed *from* the government. Yet one interviewee stated that "efforts to leverage and integrate learning from the private sector have been ad hoc, opaque, and limited. The private sector should be involved in the decision to 'raise the shield.'" However, many said that some elements of the federal government, especially some SRMAs, have been more useful than others in complementing information pushed out via Shields Up with more useful, sector-specific information, including in classified settings.

This view is not necessarily shared by the less mature players, and this raised the broader question of the ambiguity about which audience Shields Up is aiming to speak to. While the more mature and better resourced actors in the private sector may not find the information useful, at the same time Shields Up may not be reaching all the businesses and individuals who may need more foundational cybersecurity information and guidelines. The Shields Up campaign primarily targets US government agencies, critical infrastructure providers, and private companies, but many smaller businesses and individuals may not be aware of the campaign or have the resources to implement its recommendations. Relatedly, the international dimension of Shields Up has largely gone unacknowledged by the government but that plays an important role in the credibility of the campaign. "Cybersecurity is a global environment," said one interviewee, "and many elements of the private sector in the US are multinational. But it is not clear if the government is considering how Shields Up messaging may resonate not only domestically, but also abroad."

Finding 13:

Shields Up reveals the role of time and the challenges associated with long-term warning.

Finally, Shields Up reveals the challenges associated with long-term warning, especially for situations in which anticipated cyber incidents have not taken place. One consistent issue that many interviewees raised was the problem of "vigilance fatigue." Many made negative comparisons to the DHS color-coded terrorism alert levels, noting that it can be politically challenging to determine when to bring the "shields down," thereby rendering the designation itself meaningless. The longtime horizon of Shields Up contributes to this issue. As one interviewee reflected, "What does Shields Up mean over a year into the war? How do we handle a long-lasting warning problem? We cannot expect full mobilization for an indefinite period of time." Others noted that some of the big tech firms, such as Microsoft and Google, have been issuing warnings about Russian cyber threat activity, but there has not been a corresponding warning coming from Shields Up. "If these firms are right," one interviewee said, "then theoretically the shields should be powered up again."

This confusion suggests the need for clearer criteria for which events trigger a "Shields Up." While there is an ongoing debate about the relative lack of significant cyber attacks against the US or NATO during the Ukraine war, this lack does not mean threats will not materialize in the future in the context of this conflict. However, as the Shields Up campaign is currently constituted, it does not identify the conditions under which cyber risks may increase or change as the dynamics of the geopolitical environment changes. Russia continues to create risk, but many in industry perceive that they are not continuing to receive information from the federal government on this issue. One noted that "Shields Up is not updated on a routine basis. Just because nothing has happened yet does not mean that it isn't important to know the risk and threat environment and how these are changing."

V. RECOMMENDATIONS

Drawing on the above findings, the task force developed four key recommendations, along with several supporting recommendations. The proposed recommendations do not aim to overhaul how the federal government is organized or systematically rework how it engages with the private sector. Instead, we aim to provide recommendations that will have the greatest leverage in addressing the gaps and challenges identified in the findings. A core issue across the findings is that the US government typically has had three ways of interacting with the private sector: as a purchaser, regulator, or law enforcer. Yet none of these models is a good fit for operational collaboration.Therefore, our goal is to help define new ways of thinking about public-private collaboration beyond existing models.

Table 2, below, illustrates how the recommendations map to the findings from the previous section.

Recommendation 1:

Institutionalize crisis communications within the federal government.

Multiple messages and communication channels from the government during an incident creates confusion and undermines credibility, trust, and effectiveness of response, especially when competing priorities are communicated. For the government to effectively communicate, government officials need information and facts from industry, which is most likely to have useful information, especially technical details. For this exchange to happen at scale, a "whole of system" approach is needed. Moreover, communication issues have broader implications, especially in terms of how the US government coordinates and synchronizes communication about cyber incidents that also affect its allies and partners.

The federal government has codified roles and responsibilities for its response to any cyber incident, including those that affect both the public and private sectors, in Presidential Policy Directive-41 (PPD-41). PPD-41 contains a cursory discussion of how the federal government will communicate with affected entities during times of crisis. In particular, it states that "threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available Federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other Federal Government entities."[48] As such, PPD-41 defines some role for both the Department of Justice (threat response) and the Department of Homeland Security (asset response) for government communications, but the details remain murky. Moreover, given the elevation of cybersecurity issues within the White House—to include within the NSC and via the ONCD—the federal government should update crisis communications responsibilities. Such a review should establish which entity within the federal government has the lead for crisis communication during an incident, with the understanding that the lead may vary by context. For instance, for incidents in which a UCG has been formed (as was the case with SolarWinds and Microsoft Exchange), the lead may be the White House, while it may be a different department or agency for less significant incidents. This approach will help ensure that a consistent and coordinated message is delivered to the public and other stakeholders, improving the credibility, coherence, and effectiveness of response.

One of the reasons that the US government struggles with communications is that agencies usually have a specific audience that aligns with their mission. Our recommendations do not suggest that only one agency should communicate during a cyber incident. Instead, our emphasis is on coordination. Better coordinated messaging is in the interests of all government agencies, as this will substantially boost credibility with the private sector.

Below are several supporting recommendations that would further improve crisis communications around cyber incidents:

Table 2: Mapping Recommendations to Findings

Recommendations	Findings
Recommendation 1: Institutionalize crisis communications within the federal government.	**Finding 1:** There has been significant progress in operational collaboration over the past decade. **Finding 2:** Challenges of trust in the federal government are enduring and multifaceted, lacking a whole-of-society approach. **Finding 3:** The federal government faces challenges of effective crisis communication and coordination of messaging to the private sector. **Finding 8:** There was a lack of transparency on the part of the federal government about thresholds for responses in the Colonial Pipeline incident.
Recommendation 2: Ensure that there are professional incentives and opportunities for collaboration between the federal government and industry with the right people in the room.	**Finding 2:** Challenges of trust in the federal government are enduring and multifaceted. **Finding 7:** The ways in which SolarWinds impacted the federal government affected collaboration and trust. **Finding 9:** Colonial Pipeline revealed a need for greater regulatory focus and guidance pertaining to cybersecurity and resilience—along with a need for expertise and capacity.
Recommendation 3: Incorporate state and local stakeholders into operational collaboration.	**Finding 4:** There is uncertainty about how a growing regulatory footprint will affect operational collaboration. **Finding 5:** Effective operational collaboration often depends on size and maturity level, which is mismatched with the expectation that the federal government treats all companies equally.
Recommendation 4: Establish a joint cyber warning center within the intelligence community that includes public and private sector elements.	**Finding 6:** The nature of the SolarWinds incident—its attack vector and scale—posed unique challenges. **Finding 10:** Shields Up represents a potential use case of early warning. **Finding 11:** The objectives of the Shields Up campaign lack clarity. **Finding 12:** Many questioned the utility of information being shared and noted ambiguity about who the audience for Shields Up is. **Finding 13:** Shields Up reveals the role of time and the challenges associated with long-term warning.

- **Supporting Recommendation 1.1: Define the role of the UCG in crisis communications.** Given that the UCG is the primary mechanism to coordinate the federal government's response to a significant cyber incident, any review of roles and responsibilities for crisis communications should explicitly address the role of the UCG. This review could result in more specificity with respect to how and with whom different categories of information can be shared.

- **Supporting Recommendation 1.2: Streamline industry outreach to and communication with the government.** Just as industry would benefit from having a single point of contact and communication with the government, industry also needs a coordinated outreach plan to the government. Oftentimes, such outreach is ad hoc and depends on interpersonal relationships. Therefore, private sector incident response plans should clarify who

is authorized to reach out to various government entities, and a coordinated outreach plan should be included in industry playbooks to avoid various individuals reaching out in a way that is not coordinated or consistent (or potentially counterproductive). Playbooks should include guidance on how industry and government can work together effectively during a cyber incident. They should also contain specific information and instructions for what can be shared, in what order, and with whom. Having a streamed outreach process will be even more important for industry as the regulatory landscape changes and reporting requirements grow.

- **Supporting Recommendation 1.3: The federal government should develop transparent options and scenarios for when and how the private sector—affected entities as well as cybersecurity and IT companies—should be incorporated into a UCG.**
  Recent cyber incidents have seen the private sector incorporated into UCGs, although the criteria, process, and nature of the private sector's role remains opaque. Therefore, how and when the private sector is incorporated into UCG, the expectations of private industry's participation, and the crisis communications implications should be clarified. This recommendation has implications for crisis communication as well as broader implications for promoting transparency and trust.

- **Supporting Recommendation 1.4: Apply a nodal approach to crisis communications.**
  It is impossible for the US government to have a 1:1 relationship with every firm. Therefore, it will need to take a nodal approach to communication—consistent with the recommendations of the second NYCTF report—so that information can efficiently flow down from the government to appropriate entities. This approach may mean developing procedures for crisis communication that rely on key cybersecurity enablers and nodes, such as the Cyber Threat Alliance, the Analysis & Resilience Center for Systemic Risk, sector-specific ISACs, Sector-Coordinating Councils, and so on, which can in turn disseminate information more broadly.

- **Supporting Recommendation 1.5: Develop crisis communications protocols that take into account varying scopes of cyber incidents.**
  The government should establish protocols for crisis communication across different types of incidents, identifying in advance potential communications issues or considerations for scenarios in which the government is both the target and responder to private-sector victims; for when the incident only affects the government; and for when it only affects the private sector. This will be driven in part by an understanding of where and how attacks can manifest risks across critical infrastructure. Communications for each kind of incident and scope should be incorporated into the new plan for cyber incident response, perhaps as an annex. This should also drive the specific nodes that are activated to participate in such a plan, as the relevant nodes will vary depending on the scope of the incident.

- **Supporting Recommendation 1.6: Cyber Safety Review Board retrospective reports should explicitly address crisis communications issues.**
  The CSRB was established to review major cyber incidents and make concrete recommendations for improving cybersecurity. Therefore, future CSRB reports should also evaluate the effectiveness of crisis communications in incidents being examined. CSRB retrospective reports should identify lessons learned in a particular incident about crisis communications, which should be incorporated into best practices going forward. As of this writing, Congress is developing a legislative proposal to, among other things, codify the CSRB and provide it with additional authorities. Such legislation should include a provision requiring the CSRB to evaluate crisis communications in its reports.

- **Supporting Recommendation 1.7: Improve federal government transparency around counter-ransomware actions and thresholds for federal government responses.**
  The federal government should more clearly communicate its criteria for its approaches to ransomware groups and share information in a way that enables industry to prioritize ransomware threats, given their ubiquity. In some instances, the federal government may not be able to share sufficient information to support prioritization, but it should be transparent regarding what data can and cannot be communicated.

Recommendation 2:

Ensure that there are professional incentives and opportunities for collaboration between the federal government and industry with the right people in the room.

Another theme running through the case studies and the findings is that people, expertise, and interpersonal relationships serve as the foundation for effective collaboration and the linchpin for cultivating trust. Indeed, this theme is underscored in the 2023 National Cyber Workforce and Education Strategy.[49] Trust and collaboration between industry partners and the US government needs to be established in person and from the ground up—at the working level, not just between senior leaders and executives. Both government and industry stakeholders need to know that they are collaborating with a competent, skilled, and trustworthy interlocutor. However, information-sharing and collaboration are not in anyone's job description—it is not a core duty within the government or the private sector. Without formalized career incentives, collaborative relationships simply rely on the goodwill of committed professionals. Career incentives would assist, for example, in making the JCDC truly a "joint" entity with meaningful participation by relevant stakeholders across the interagency, especially within the intelligence community. Therefore, both the government and industry should create career incentives and opportunities for collaboration.

Below are several supporting recommendations of specific measures to create professional incentives for collaboration:

- **Supporting Recommendation 2.1: Update job descriptions to include information-sharing and collaboration, and create career incentives to participate in these activities.**
  Information handling (requesting, sharing, collecting, disseminating) and operational collaboration should be clearly identified responsibilities within job descriptions of identified roles in both the government and the private sector. Drawing inspiration from the 1986 Goldwater-Nichols Act, which led to significant changes in officer career development within the Armed Forces, both the public and private sector should also create specific, tangible career incentives for collaboration. This would make collaboration not simply another duty assigned on top of core responsibilities but in fact a core duty. For example, individuals could be given professional credit or incentives for time spent working jointly and collaboratively; or "joint" time could be a requirement for promotion within certain key roles. This requirement would also entail developing the right set of tools to measure performance on specific collaboration criteria.

- **Supporting Recommendation 2.2: Update the Intergovernment Personnel Act (IPA) Mobility Program.**
  Under the auspices of the Office of Personnel Management (OPM), the IPA program "provides for the temporary assignment of personnel between the federal government and state and local governments, colleges and universities, Indian tribal governments, federally funded research and development centers, and other eligible organizations."[50] Departments and agencies utilize this program, which is far less restrictive and costly than is direct federal government hiring, to make up for key talent shortfalls or temporarily bring in outside talent and expertise to address specific issues. Key entities within the federal government should review and, where possible, explore opportunities to update the IPA program to create opportunities for temporary appointments within the federal government from industry, specifically for technical fields. This approach should be part of a broader process to identify mechanisms for improving technical expertise within the US government, especially around operational technology.

- **Supporting Recommendation 2.3: Clarify the criteria for participation in the JCDC.**
  The criteria for which entities are able to participate in the JCDC and the rationale behind those decisions are currently opaque. As a result, the current membership seems arbitrary. Therefore, DHS should develop (or release, if they already exist) the criteria for decisions about inclusion or exclusion of entities in the JCDC. A rule set to which DHS can point would help to improve credibility and transparency.

- **Supporting Recommendation 2.4: Create executive education programs focused on operational collaboration.**
  Senior leadership programs can help socialize the importance of collaboration in responding to cyber threats and risks, as well as fostering trust and transparency. For example, government officials have increasingly engaged the technical and hacker communities by actively participating in industry events, such as the DEF CON and Black Hat conferences. Establishing and resourcing executive educational and other formal programs for leaders in government, as well as business leaders—

including board directors, c-suite, and other executives in the private sector—would improve education about operational collaboration and create opportunities for cross-pollination with cyber professionals.

- **Supporting Recommendation 2.5: Build capacity to cultivate a culture of collaboration at scale for the next generation.**
  Professional certifications provide an opportunity to inculcate normative standards into the talent space at earlier stages of professional development. Therefore, professional certifications, such as CompTIA, ISC2, and others, should include a module that certifies professionals in foundational knowledge and expertise necessary for operational collaboration. Additionally, continuing professional education requirements could include participating in government and private sector workshops and conferences.

Recommendation 3:

Incorporate state and local stakeholders into operational collaboration.

The National Cybersecurity Strategy calls for the federal government to coordinate and tightly integrate its incident response efforts with state and local stakeholders, and to provide support when those entities are affected by threats such as ransomware. While this core idea resonates with many of the themes we uncovered in our outreach efforts, the strategy is largely silent on how the federal government will operationalize collaboration with state and local actors. The reality is that operational collaboration is often depicted as a bilateral relationship between the federal government and the private sector, but in practice it is a multilateral one that often involves state and local actors. Moreover, the federal government does not have the capacity to conduct incident response at scale for all state and local victims. State and local governments also vary significantly in cyber capability. Therefore, in operationalizing the concepts within the National Cybersecurity Strategy around collaboration with state and local actors, the federal government should take into account the significant variation across state and local actors in terms of their resources, maturity, capacity for operational collaboration, and so on.

Below are several supporting recommendations that provide examples of how to improve collaboration with state/local actors:

- **Supporting Recommendation 3.1: Incorporate the most mature and capable state and local actors into existing federal collaboration structures, such as the JCDC and Cyber Unified Coordination Group.**
  More mature state and local actors are better positioned and have the capabilities and willingness to engage with the federal government and industry for routine operational collaboration; these entities can both benefit from and contribute to systematic information-sharing programs.

- **Supporting Recommendation 3.2: State and local actors should assess the feasibility of putting private cybersecurity firms on retainer for incident response.**
  Such a vehicle could help surmount some of the issues with expertise and capacity within state and local actors to conduct incident response and alleviate some of the challenges of drawing on federal government resources for incident response, which are already stretched thin. This approach would ensure that state and local victims receive the necessary support and expertise to effectively respond to cyber incidents.

- **Supporting Recommendation 3.3: Incorporate state and local entities into crisis communications plans and define their roles and significance.**
  Crisis communications and coordination should include protocols, plans, and procedures for working with affected state and local entities, when relevant, to ensure that messaging is consistent across various levels of government.

- **Supporting Recommendation 3.4: Clarify the relationship between the MS-ISAC, JCDC, and DHS/CISA in terms of how to incorporate state/local actors.**
  State and local actors are often encouraged to engage with the MS-ISAC as a means of collaborating with the broader federal government. However, it is not clear that state and local players see a significant benefit in this relationship, nor is the federal government's relationship with the MS-ISAC well-defined.

- **Supporting Recommendation 3.5: Define roles and responsibilities for state/local government when DHS declares a significant cyber event that impacts states and local actors.**
  DHS should clarify the process for prioritization of federal government responses during significant cyber events and involve state and local entities to help inform that prioritization, especially for incidents that impact both state and local government functions.

Recommendation 4:

Establish a joint cyber warning center within the intelligence community that includes public and private sector elements.

Russia's invasion of Ukraine and CISA's decision to stand up the Shields Up campaign reveal the importance of cyber warning. While the concept of early warning draws on longstanding and robust literature, it has not yet been fully explored in the context of cybersecurity. Warning is different from forecasting, in that a warning incorporates real-time and evolving data to indicate a near-time possibility of a cyber incident. Warning helps avoid strategic surprise. Many cyber incidents are triggered by geopolitical events outside of cyberspace. However, no US government agency is responsible for providing cyber warning to the private sector. Moreover, most entities in the private sector are not connecting what is taking place in cyberspace with the broader geopolitical environment. Any warning should be clear about what the recipients of such information are expected or requested to do as a response. The success of warning should be measured in terms of the reduction of uncertainty for defenders or enabling better resource allocation. Our task force devotes a more detailed treatment to this issue in Appendix 1 of this report.

- **Supporting Recommendation 4.1: Create a joint warning center that is truly joint.**
  A joint cyber warning center should be truly joint in that it should encompass the intelligence community, SRMA representatives, other elements of the federal government as appropriate (such as CISA), representatives from critical infrastructure (including firms themselves and sectoral-based organizations), and critical cybersecurity enablers (such as cloud service providers, cybersecurity firms, and nonprofit organizations). This joint warning center should reflect a nodal model, as described above, where specific nodes can be activated to distribute information about warning to broader audiences.

- **Supporting Recommendation 4.2: Ensure that a warning center has an advocate within the intelligence community; consider attaching to the Cyber Threat Intelligence Integration Center (CTIIC) within the Office of the Director of National Intelligence (ODNI).**
  Given that warning is inherently intelligence driven, the center should have an advocate and a single coordinator within the intelligence community who can empower SRMA representatives and engage the right partners across critical infrastructure sectors. The intelligence community will also have to devote a dedicated funding stream to this effort. A warning center could be attached to CTIIC within the ODNI. However, there could be benefits to physically locating the center (or centers) outside of Washington, D.C., where the customers are located. Policymakers should further consider the concept of nodes or hubs, as detailed in the second NYCTF report to facilitate rapid mobilization of relevant actors for specific issues or contingencies.

- **Supporting Recommendation 4.3: A warning center should be focused on providing warning to the most essential elements of critical infrastructure.**
  It is important to define the consumers of warning because many organizations lack the capacity to act on a warning directly. Our task force proposes to start a cyber warning effort with the target entities the most critical of critical, being the subset of critical infrastructure companies where a cyber incident could cause catastrophic damage to national security, the national economy, or public health and safety. Currently, the federal government has identified such entities under Section 9 of Executive Order 13636 (which is why these companies are referred to as "Section 9" firms), but the warning targets should expand as this list evolves into other forms, such as Systemically Important Entities. The federal government could pilot a warning center with the financial services sector as an initial test case.

- **Supporting Recommendation 4.4: Smaller entities should incorporate into vendor contracts provisions for situations involving heightened warning/awareness.**
  One challenge faced by many small to medium-sized firms is a lack of a dedicated cybersecurity staff. As a result, these entities often rely on contracts with third-party IT vendors to assist in routine cybersecurity management as well as incident response. At the same time, a critical gap in current warning initiatives is the ability of smaller entities to digest and use information shared by the government. To ensure during times of heightened risk that these small to medium-sized firms are receiving helpful information to enable effective decision-making, such firms should find mechanisms to update or include in contracts with IT vendors provisions that set expectations and define criteria for their role.

VI. NEXT STEPS

Moving forward, the NYCTF will engage with key leaders across all levels of the government, private sector, and broader cybersecurity community to advocate for strengthening operational collaboration and bridge the gap between industry and government via implementing the recommendations suggested in this report. Specifically, the task force will drive toward improving communication and transparency, addressing workforce and personnel challenges, incorporating state and local partners, and establishing a joint warning capability within the US government. In doing so, the task force will also look to advance the report's findings in the context of the implementation of the 2023 National Cybersecurity Strategy; many of the themes that define that strategy are deeply resonant with the findings and recommendation of this task force report. The NYCTF will continue to advocate for a more defensible cyberspace and the implementation of new models of operational collaboration.

APPENDIXES

Appendix 1: Considerations for an Early Warning Framework

Types of Warning

In establishing a warning center, policymakers should consider that warning can occur at different levels of analysis, from the tactical to the operational to the strategic, and that different stakeholders may have comparative advantages in providing different types of warning. Tactical warning typically takes place at high levels of specificity about a particular threat actor and/or target that involves an immediate action. Tactical warning may be more likely to come from industry partners and/or private sector sources, such as major cybersecurity providers. Operational warning aimed at day-to-day decision-making of potentially affected entities is likely to be broader in scope, such as threats to a specific critical infrastructure sector. Finally, strategic warning involves longer time, over the horizon threats that leaders at the CEO and investor level should incorporate into their posture and understanding of the threat environment. The government, via the intelligence community, is likely to have a comparative advantage in providing such strategic warning.

The level of analysis of warning is deeply related to the time horizons of warning. In particular, it will be important to distinguish between early warning, standing warning, and emergent warning. Early warning is often associated with nuclear warning during the Cold War and systems such as the Distant Early Warning (DEW) line, which was a system of radar stations that aimed to detect potential incoming Soviet bombers. The logic of early warning is to provide sufficient advance notice of a forthcoming attack to enable defenders to take actions to prevent it or mitigate its consequences. However, there are questions as to whether early warning is possible in cyberspace and, therefore, whether alternative forms of warning (such as concurrent warning) are more appropriate for the digital domain.

Distinct from early warning, standing warning refers to situations that are expected to last for long periods of time (potentially years). Many cyber challenges fall into the category of standing warning. This form of warning depends on continuous monitoring of particular threats. Transparency and communication are particularly important for standing warning—even if there is no change in the threat environment. In other words, communicating the absence of warning is important information for consumers.

Finally, emergent warning problems occur when a particular geopolitical situation (e.g., a crisis between the US and China over Taiwan) or issue (e.g., the emergence of ransomware), which was not previously anticipated, prompts a change in the threat picture. This form of warning is especially important for cyber threats because cyber incidents are often linked with geopolitical events. However, many private-sector entities do not connect what is taking place in cyberspace with the broader geopolitical environment. Since the private sector is not naturally attuned to these issues, the government could play a crucial strategic warning role. Shields Up is a good example of an emergent warning problem (i.e., Russia is likely to conduct cyber attacks against the West in the context of its invasion of Ukraine) that has evolved into a standing warning problem now that the war is ongoing. Thinking carefully about the time horizons of warning and what specific behavior such warning is meant to elicit is therefore critical.

Jointness

A joint cyber warning center should be truly joint—it should be conceived of as a jointly managed and executed process that involves both public and private stakeholders. This would require a number of actions on both sides.

On the government side, truly joint warning requires reconceptualizing how the intelligence community thinks about the consumers of intelligence products and the role of the private sector. Without input from the private sector about what indicators and warnings the intelligence community should be looking for, a

cyber warning program is not likely to be effective. On the other hand, in many cases the main beneficiaries of warning will be private entities. Under this conceptual framework, the intelligence community will have to treat critical infrastructure companies—however policymakers ultimately define this subset of the private sector—as both consumers of intelligence and generators of intelligence requirements. Furthermore, the IC will have to dedicate funding to this effort.

On the private sector side, industry should self-organize. Building on the prior NYCTF report's concept of cyberspace as a system of nodes, each sector should establish its own node to serve as a liaison with the intelligence community. This structure will help drive prioritization of critical infrastructure intelligence requirements within the intelligence community and make the number of entities involved manageable. The financial services sector is an important test case of this concept. In many ways, the sector's ability to work with the intelligence community has been facilitated by the most critical entities within the sector choosing to self-organize, establishing a "node" via the Analysis and Resilience Center (ARC), as well as the maturity and competence of the sector and the ARC. Effective collaboration requires that all parties show up with appropriate and competent individuals—yet there is significant variation in maturity and capacity across critical infrastructure sectors.

Consumers of Warning

A consistent theme in the Shields Up case study was the lack of clarity around who the consumers of warning are. In general, potential warning consumers could range from individuals to small/medium enterprises to large companies, or from businesses in general to specific critical infrastructure subsectors, with the possibility of further refining these categories into various subsets. A lack of clarity concerning who the consumer is and what their needs are risks making information provided insufficiently specific or relevant to be useful or actionable by the desired consumer. Therefore, it is imperative to clearly define who the consumer is. Our task force proposes to start a cyber warning effort with the core of the warned entities being national assets/critical infrastructure—the most critical of critical as an initial set of consumers of warning.

The private sector should be proactive in this regard, defining its obligations as part of participating in a potential warning program. Specifically, each sector should identify which firms, assets, or entities should be defined as the most critical, establish a transparent process for making such identifications, and periodically reevaluate the classifications. Industry itself is best positioned to do so, rather than waiting for the government.

The Purpose of Warning

In addition to defining the consumers of warning, a central challenge is defining the purpose of warning. Unlike other domains, warning specific potential targets with enough lead time to put in place adequate countermeasures to ride out a cyber incident or to stop it entirely is unlikely. Because cyberspace is a nodal network that operates at light speed, the best outcome any warning system can likely achieve is to warn similarly situated entities such that they could be affected by the same threat and how they can mitigate it. The goal of warning, therefore, should be to provide such defenders enough time to take the necessary countermeasures and implement compensating controls. In other words, information shared as part of warning should be clear about what the recipients of such information are expected or being asked to do as a result. The key question to making warning effective is to define in advance and with some level of specificity what actions the consumers of warning should take.

Warning involves an element of probability or uncertainty, and it inevitably comes with confidence intervals. There is an element to warning that involves being aware that a situation is worsening, even if an attack is not underway. Moreover, even if an adverse event ultimately does not transpire, this lack does not mean the warning was wrong. Under this framework, warnings should include some level of specificity to differentiate them from general awareness about the threat environment.

Another significant issue with warning is extracting the signal from the noise. There is a deluge of information about the threat environment in cyberspace, which makes identifying meaningful indicators difficult. The government can play a critical role in this area by helping to provide context and enabling prioritization.

Measuring Success

It will be tempting to define successful warning as predicting attacks. However, this definition risks setting the bar impossibly high in a cyber context. Instead, successful warning should be conceptualized as reducing uncertainty for defenders or enabling better resource allocation. Moreover, warning will be a learning process that improves over time. The financial services sector, for reasons enumerated above, will be an important prototype for how such a warning system could work. If successful outcomes are not possible for that sector, this result would indicate that warning will not be effective more broadly.

Appendix 2: Sample Interview Questions

Below is a set of sample interview questions that informed the NYCTF's key findings and recommendations. These questions were used during in-depth interviews with industry to gain insights into each case study.

SolarWinds

1. What were the criteria/thresholds for government steps taken for public vs. the private sector? Was the government perceived as responding differently to public vs. private victims?
2. What was the role of Congress in this incident and how did it impact collaboration?
3. As a counterfactual exercise, would the USG go public with its announcement if the private sector hadn't discovered it first and chose to communicate it?
4. Are there protocols in place for when the USG is both itself the target and trying to respond to victims in the private sector?
5. During a widespread breach like SolarWinds, what is the best way to incorporate the private sector in the communication and decision-making process?

Colonial Pipeline

1. What was your role in the case (if any)? Can you provide your specific insights on what went well and what could have been done better in terms of mitigation strategies during/after the incident?
2. What were the criteria for government involvement in this case compared to other similar ransomware cases where the government did not take extensive action? Especially post payment of ransom by the CEO? What kind of precedence did this set for cyber incidents at large?
3. In the wake of Colonial, what implicit or explicit expectations did the government set for industry in its response actions? Are these responses repeatable/scalable? Are there clear and transparent criteria for when similar entities can expect similar levels of government support? How widely is this level of collaboration and resources help applicable to other sectors and industries?
4. Who is providing expertise to federal agencies with regulatory authority over privately owned critical infrastructure? Specifically with respect to Colonial Pipeline, who/which agencies were involved in decision-making and implementation of mitigation strategies?

Shields Up

1. How effective has Shields Up been?
2. What does it mean to be "Shields Up"? Does industry understand the goals/purposes of Shields Up? How is this different from what companies are already doing?
3. What happens if a Shields Up incident actually happened in the context of Ukraine?
4. If no major cyber incident occurs, how will we know if this is an example of successful operational collaboration?
5. Will vigilance fatigue erode trust and credibility in the government?
6. What is the private sector's perception of efforts related to Shields Up, such as the JCDC and recent CIRCIA legislation?
7. Does industry perceive the information being pushed out by the government as useful?

NOTES

1. Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," NPR, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

2. Sam Shead, "Microsoft's Exchange Hack: Everything You Need to Know," CNBC, March 9, 2021, https://www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html

3. Jenna McLaughlin, "Companies Scramble to Defend Against Newly Discovered Log4j Digital Flaw," NPR, December 14, 2021, https://www.npr.org/2021/12/14/1064123144/companies-scramble-to-defend-against-newly-discovered-log4j-digital-flaw

4. Dina Temple-Raston, "Colonial Pipeline CEO Explains the Decision to Pay Hackers $4.4 Million Ransom," NPR, June 3 2021, https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom

5. Greg Myre, "JBS Cyberattack Just the Latest Major Company to Be Shut Down by Hackers," NPR, June 2, 2021, https://www.npr.org/2021/06/02/1002604418/jbs-cyberattack-just-the-latest-major-company-to-be-shut-down-by-hackers

6. The Associated Press, "Scale, Details of Massive Kaseya Ransomware Attack Emerge," NPR, July 5, 2021, https://www.npr.org/2021/07/05/1013117515/scale-details-of-massive-kaseya-ransomware-attack-emerge

7. "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

8. "National Cybersecurity Strategy 2023," The White House, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

9. "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)," CISA, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

10. "The 2017 New York Cyber Task Force, Building a Defensible Cyberspace," Columbia SIPA, https://www.sipa.columbia.edu/global-research-impact/initiatives/cyber/nyctf/defensible-cyberspace

11. "2020 New York Cyber Task Force, Enhancing Readiness for National Cyber Defense through Operational Collaboration," Columbia SIPA, https://www.sipa.columbia.edu/global-research-impact/initiatives/cyber/nyctf/operational-collaboration

12. Microsoft Threat Intelligence, "Analyzing Solorigate, the Compromised DLL File That Started a Sophisticated Cyberattack, and How Microsoft Defender Helps Protect," Microsoft Security Blog, December 18, 2020, https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

13. "Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government," The White House, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

14. "Joint Statement Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure," CISA, January 5 2021, https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

15. Fireeye, "Evasive Attacker Leverages SolarWinds Supply Chain Compromises with SUNBURST Backdoor," Mandiant, December 13, 2020, https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

16. Jeff Stone, "FireEye Ties SolarWinds Hack to Russia with Postcard Delivered to CEO's Home," CyberScoop, June 15, 2021,

https://cyberscoop.com/fireeye-russia-solarwinds-kevin-mandia-postcard/

17. [#14] "Joint Statement Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure," CISA, January 5 2021, https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

18. Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo "Broken Trust: Lessons from Sunburst," Atlantic Council, Mar 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/

19. "Colonial Pipeline Cyber Incident," US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, May 13, 2021, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

20. "Pipeline Hack," The New York Times, May 14, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. "DarkSide Ransomware Colonial Pipeline Response," Wired, https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/

21. "FBI Statement on Compromise of Colonial Pipeline Networks," FBI, May 10, 2021, https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

22. "Remarks by President Biden on the Colonial Pipeline Incident," The White House, May 13, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/#:~:text=My%20administration%20is%20continuing%20to,we%20know%20what%20they%20need

.23. "Joint CISA-FBI Cybersecurity Advisory: DarkSide Ransomware," CISA, May 11, 2021, https://www.cisa.gov/news-events/alerts/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware

24. "US to Announce Recovery of Millions from Colonial Pipeline Ransomware Attack," Reuters, June 7, 2021, https://www.reuters.com/business/energy/us-announce-recovery-millions-colonial-pipeline-ransomware-attack-2021-06-07/#:~:text=WASHINGTON%2C%20June%207%20(Reuters),disruptive%20US%20cyberattack%20on%20record

25. "Biden warns Russia's Putin about ransomware attacks from his country, says US will respond if they don't stop," The Washington Post, July 9, 2021, https://www.washingtonpost.com/politics/russia-united-states-ransomware-attacks-biden/2021/07/09/034ac07e-e0d7-11eb-b507-697762d090dd_story.html

26. "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

27. "Press Briefing by Press Secretary Jen Psaki and Deputy NSA for Cyber and Emerging Technologies Anne Neuberger, March 21, 2022," The White House, March 21, 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/21/press-briefing-by-press-secretary-jen-psaki-and-deputy-nsa-for-cyber-and-emerging-technologies-anne-neuberger-march-21-2022/

28. David Uberti and Catherine Stupp, "Colonial Pipeline Hack Sparks Questions About Lax Cyber Oversight," The Wall Street Journal, May 10, 2021, https://www.wsj.com/articles/colonial-pipeline-hack-sparks-questions-about-lax-cyber-oversight-11620689340

29. "Security Directive Pipeline 2021-01B," Transportation Security Administration, May 29, 2022, https://www.tsa.gov/sites/default/files/sd_pipeline-2021-01b_05-29-2022.pdf

30. "TSA Updates, Renews Cybersecurity Requirements for Pipeline Owners," Transportation Security Administration, July 26, 2023, https://www.tsa.gov/news/press/releases/2023/07/26/tsa-updates-renews-cybersecurity-requirements-pipeline-owners

31. "Shields Up," CISA, https://www.cisa.gov/shields-up

32. David Jones, "CISA Director Urges Businesses to Own Cyber Risk," Cybersecurity Dive, March 24,2023, https://www.cybersecuritydive.com/news/cisa-director-urges-businesses-own-cyber-risk/645932/

33. "NACD and ISA Launch 2023 Cyber Risk Oversight Handbook Featuring CISA and FBI," NACD, March 22, 2023, https://www.nacdonline.org/about/NACD-in-the-news/press-release/nacd-and-isa-launch-2023-cyber-risk-oversight-handbook-featuring-cisa-and-fbi/

34. [#31] "Shields Up," CISA, https://www.cisa.gov/shields-up

35. "CISA Establishes Ransomware Vulnerability Warning Pilot Program," CISA, March 13, 2023, https://www.cisa.gov/news-events/news/cisa-establishes-ransomware-vulnerability-warning-pilot-program

36. "CISA Launches New Joint Cyber Defense Collaborative," CISA, August 5, 2021, https://www.cisa.gov/news-events/news/cisa-launches-new-joint-cyber-defense-collaborative

37. Rebecca Klar, "CISA Director: US Needs to Be Vigilant, Keep Our Shields Up Against Russia," The Hill, January 5, 2023, https://thehill.com/policy/technology/3801077-cisa-director-us-needs-to-be-vigilant-keep-our-shields-up-against-russia/

38. "Shields Up: Easterly, Inglis Op-ed," CyberScoop, June 6, 2022, https://cyberscoop.com/shields-up-easterly-inglis-op-ed/

39. "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents," GAO-22-104746, January 13, 2022, https://www.gao.gov/products/gao-22-104746; Federal Response Group to Microsoft Hack Features Private Sector Firms, March 17, 2021, https://www.meritalk.com/articles/unified-coordination-group-microsoft-hack-private-firms-solarwinds/

40. "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

41. "US Cyber Review Punts on Russian Hack, Hinting at Limitations," Bloomberg, November 16, 2022, https://www.bloomberg.com/news/newsletters/2022-11-16/us-cyber-review-punts-on-russian-hack-hinting-at-limitations https://www.nextgov.com/cybersecurity/2022/07/cyber-safety-review-board-closes-book-solarwinds-while-reporting-log4j/374220/

42. According to reporting from NextGov, the DHS spokesperson provided the following explanation: "Given the various reviews that both the federal government and the private sector conducted of the Solar Winds compromise over the past year, the White House and the Department of Homeland Security have determined that the best use of the Cyber Safety Review Board's expertise is to focus its initial review on the vulnerabilities in log4j software library and associated remediation process." "New Cyber Safety Board Pivots to Tackle Log4j Vulnerabilities," NextGov, February 2022, https://www.nextgov.com/cybersecurity/2022/02/new-cyber-safety-board-pivots-tackle-log4j-vulnerabilities/361626/

43. Mike Elgan, "Colonial Pipeline: Federal Regulation Update," Security Intelligence, July 11, 2022, https://securityintelligence.com/articles/colonial-pipeline-federal-regulation-update/

44. Kimberly Wood, "Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack," Georgetown Environmental Law Review, March 7, 2023, https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/

45. "Executive Order (EO) 14028—Improving the Nation's Cybersecurity," GSA, https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/technology-products-services/it-security/executive-order-14028#:~:text=Executive%20Order%20(EO)%2014028%20%2D,and%20software%20supply%20chain%20integrity

46. "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," DHS, July 20, 2021, https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators#_blank

47. "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," DHS, May 27, 2021, https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

48. "Presidential Policy Directive—United States Cyber Incident Coordination," The White House, July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

49. "NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY," Unleashing America's Cyber Talent, The White House, July 31, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

50. IPA Mobility Program, US Office of Personnel Management, "Intergovernment Personnel Act," OPM, https://www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/

SIPA CYBER PROGRAM
SIPA.COLUMBIA.EDU