ISAO Standards Organization

ISAO SO Special Publication 6001: Enabling Private-Public Partnerships (PPPs) for Information Sharing

v1.0

November 17, 2020

ISAO SP 6001

Enabling Private-Public Partnerships for Cyber Information Sharing

A Framework for Cross-Sector Collaboration to Advance Community Cybersecurity

Version 1.0

ISAO Standards Organization

November 17, 2020

Acknowledgements

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) in conjunction with representatives from the private, professional, and government communities in an ongoing effort to produce a unified, voluntary set of guidelines for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization

Gregory B. White, Ph.D.
ISAO SO - Executive Director
Director, UTSA Center for Infrastructure Assurance and Security

Jeremy J. West
ISAO SO – Director of Lifecycle Development
UTSA Center for Infrastructure Assurance and Security

Working Group 6— Government Relations

Work Group Chairs

Douglas M. DePeppe
Board President, Cyber Resilience Institute
Founder, eosEdge Legal

Mark Boggis
Cybersecurity Policy Solutions, LLC
Board Member, Cyber Resilience Institute

Work Group Authors and Contributors

Ted Sienknecht
Principal Architect, Public-Private Partnerships
The MITRE Corporation

Stuart M. Gerson
Epstein Becker & Green, PC
Board Member National Council of Registered ISAOs
Former Acting Attorney General of the United States

Erik M. Dullea, Esq.
Husch Blackwell LLP
CIPP/US, MSL Cybersecurity Law

Nicholas Sturgeon
Director of Information Security
Indiana University Health

Ricky Chitwood
Federal Aviation Administration
Aviation Safety Inspector - Air Carrier Operations
PED – Cybersecurity

David Halla
Program Manager
Johns Hopkins University Applied Physics Laboratory

Item	Version	Description	Date
1	0.98	Initial RFC	September 30, 2020
2	1.0	Initial Publication	November 17, 2020
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

Table of Contents

1 FORWARD

This 6000 – 1 ISAO issuance has been in the making nearly since the formation of the Standards Organization in 2015. Both the Government Relations Working Group, and the broader ISAO SO community, gave constant scrutiny to questions involving the useful governmental participation, the sputtering dynamic of ISAO formation and sustainment, ISAO business model refinement, market forces, education and knowledge surrounding ISAO utility, and achieving both effective definition and role balance for the Public-Private Partnership construct. Among the hardest challenges to consensus involved a wide-ranging and continuous debate transpired around the often-polarizing questions of role of government and commercialization.

The Working Group's ultimate confidence about 6000 – 1 is not that we provided complete answers; rather, we believe that this issuance will be helpful as a resource for identifying the high-level contours for the mission and construct of a Partnership for collective information sharing, which involves both public and private sector partners.

Along the path to 6000 – 1, Issuance 600-2 described a role of government, at all levels, intended to "enable, support and appropriately partner" with ISAOs. This phrase has served as a compass for subsequent writings of the Working Group. Yet, still unable to define or determine the proper role balance for the ideal Public-Private Partnership, the Working Group next decided that the pathway toward ISAO adoption could be found through state-level vision and support. Hence, Issuance 600 – 1 emerged from the belief that, whereas municipalities lacked the resources and knowhow to instantiate and promote widespread ISAO creation, state-level support presented a more viable next step option.

During the production of 600 – 1, however, the Working Group expressly committed to avoid characterizing 600 – 1 as a government-only institution. In various sections in the document, private sector equities were explicitly included. Thus, the Working Group was carefully attentive to the need to express information sharing as a collective responsibility and benefit, and a capability that was needed across society. Moreover, the Working Group expressly committed to producing a companion document, having a placeholder set-aside as "6000 – 1", specifically to present "the private sector" view of the partnership.

6000 – 1 indeed describes the private sector view of information sharing with a bold whole-of-society scope of the mission. The Working Group acknowledges that some readers might misinterpret our term "Private-Public Partnership", and the occasional use of the term "commercialization", as occupying the privatization path – that is, for government to step aside from an industry-led market. However, 6000 – 1 does not represent such a vision. The totality of the document clearly still embraces the partnership. And critically, the Public-Private Partnership framework and Open Commons Framework™ represent the formula by which the balance of roles within the partnership can operate most effectively. This formula should serve to answer any criticism that the private sector view unduly favors industry, or fails to recognize the necessity of true partnership to solve what are shared problems..

The challenge to the Working Group, and the ISAO Standards Organization at large, has been to articulate a new partnership that best would enable ISAOs to thrive. Thriving necessarily means incorporating market forces. Issuance 6000 – 1 is our best effort to achieve the balance needed between government and industry to commercialize ISAO adoption and sustainment.

2 EXECUTIVE SUMMARY

The pervasiveness of the nation-state adversarial threat to the cybersecurity of every entity – and the challenges in mitigating such a threat with the limited resources of any single entity – drives concerned organizations to collaborate in partnerships that blend their strengths and resources toward a shared mission of improved security and safety for the partners and the public. This document defines how private-public partnerships (PPPs) can serve as a construct to drive these community-based and market-based approaches to strengthen cybersecurity. This document is intended for action-oriented leaders in any sector or role who seeks to see tangible process on protecting against cyber threats.

This document does not prescribe a specific PPP construct among information-sharing partners. Yet, the common way that Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) have tended to form – though not exclusively, and certainly not mandatorily – is by establishing an intermediary-type entity or consortium through which the partners collaborate. While this document does not rule out bilateral or multilateral arrangements directly among sharing partners, much of the guidance and observations contained herein derive from a model that is akin to a member-driven clearinghouse or trusted agent that operates the PPP. Readers might glean useful information for establishment of other models but the premise of this Issuance is that the parties participate in the formation of an entity or facility separate from – but complementary to – their organic businesses.

This document extends and complements other standards and guidance such as ISAO 600-1 by addressing six major topics:

1. **Prelude** contextualizes the nature of challenges affecting cybersecurity and the rationale driving the issuance of this document.

2. **Introduction and Scope** presents the case for cross-sector collaboration, provides a brief history of PPPs, and ties this concept into ISACs and ISAOs. It defines PPPs as a cross-sector collaboration based on shared decision-making, shared resourcing, and shared benefit to partners and the public.

3. **Characterizing the Challenge** discusses the collective risks associated with cybersecurity that PPPs can be used as a tool to mitigate.

4. **Business Case** expands on the case for private-public collaboration and posits a number of benefits of PPPs including the ability to address complex problems beyond any one entity's reach, leverage the power of co-investment, and deter threat actors, among others.

5. **PPP Framework** proposes that addressing the trifecta of interest, agreement, and capability can drive success of the partnership. This section is intended to inform the planning and standup of PPPs by introducing design considerations regarding (1) Interest, which is predicated on a galvanizing shared issue and recognition that forming a PPP is a journey of trust-building and co-development; (2) Ability, which speaks to the mutually defined expectations, often codified in agreements, and the authority of each participant to enter into the partnership; and (3) Capability, which addresses the suite of services and solutions that are tailored to serve the needs of the PPP.

6. **Operating Principles** expands on the principles previously introduced as a driver of PPP success, including a sharing ethos, open licensing structures, and the ten core tenets of The Open Commons Framework™.

3 PRELUDE

In this section, we lay out the myriad issues and threats that create a need for new models of cybersecurity collaboration.

The White House promoted information sharing in 2015, as a necessary strategy for society to meet the increasingly sophisticated cyberattack landscape. Recent world and domestic circumstances, including the global COVID-19 pandemic and the concomitant alteration of the working environment, exposure of security risks in the American electoral system, intensified intrusion into both private and governmental data systems by adversaries, and civil unrest in the U.S., have magnified the need for effective whole-of-society efforts in dealing with what are likely to become structural and transitional changes in the cybersecurity environment. For example, in many sectors, both public and private, the isolation required in adapting to the pandemic has led to a significant amount of the nation's work being carried on from remote locations, most often workers' homes, and the resultant enhanced vulnerability risk of the private systems being employed. Remote work has proved both efficient and economical in many areas of the service economy and in government agencies. It is thus likely that the work environment has undergone permanent alteration, with remote work having become vastly more practicable and common, along with its related security risks.

The rest of the world is undergoing similar changes. Additionally, the economic fallout from the pandemic has disrupted supply chains, and indeed entire sectors of the economy. Pandemic-related economic effects could last for years, and will likely cause significant global destabilization. Against this backdrop, it is not surprising that malevolent opportunists are seizing opportunities motivated by both strategic and economic goals, and as a result, that the U.S. is experiencing a vastly increased number of ransomware attacks using novel algorithms and penetration methods; and beyond simple ransom, more frequent theft and resale of information encrypted by the ransomware algorithm. The rapid development of the Internet of Things (IoT), ranging from areas like medical devices to home security systems also has expanded cyber vulnerabilities throughout the economy and infrastructure. Indeed, with “ransomware as a service” taking hold, major aspects of the supply chain are being jeopardized.

At the governmental level, we are seeing ongoing evidence of adversary nation-state interference in our political and electoral systems, attempting to exploit social unrest resulting from the national examination of police practices in the wake of apparent racially-discriminatory and otherwise excessive conduct, as well as a very divisive political environment as we approach a presidential election. The nation also has experienced increased risk to the electrical grid and other public utilities, and to our hospitals and health care delivery functions.

In short, the complexity and pervasiveness of the risks to the cyber environment at every level of our nation's activities, both private and public, has put a premium on innovation and efficiency, to say nothing of the need for cooperation. Resources in government, both economic and human, are proving inadequate. Private sector resources also are being stressed as compliance with enhanced state data privacy and security laws, e.g., the California Consumer Protection Act, must be addressed. Indeed, we are in many ways on what is the equivalent of a wartime footing when it comes to national cybersecurity defense and resilience. And, as has been the case in our past conflicts, the path to success and durability of our institutions is through cooperative efforts among government, the private sector, and academia.[1]

The collaboration team assembled within the ISAO Standards Organization drafted this document with the foregoing in mind. We believe that the environment is ripe for structuring a new way and a new culture for the whole-of-society, approach to the collective risk we all face. Both intentionally and a bit tongue-in-cheek, this issuance is cast as a *private*-public partnership insofar as the private sector, in partnership with the government, is positioned to bring innovation and market forces to bear in advancing this new model. Yet, this PPP construct, notwithstanding its demonstrated success in other areas has proven elusive and challenging to accomplish. Thus, our goal with this issuance is to foster the success of these cybersecurity partnerships by illuminating the drivers of success, frameworks, and considerations that have shown to be useful in related efforts.

4 CONTEXT AND DEFINITION

In this section, we provide a brief overview of the history of PPPs and advance a definition aligned with prevailing usage.

4.1 CONTEXT

Public-Private Partnerships have increasingly been used as a mechanism to deliver broad public good. Traditionally, they have been employed for public works projects – such as the partnership that operates the Chicago Skyway toll bridge – in which a long-term, performance-based government contract allocates management and major share of risk on to the private entity.

Our premise is that a new collaborative construct, rooted in co-creation can advance both the performance of government as well as US economic growth and cyber resiliency. This leads to a natural application of partnership-driven approaches to address much broader problems. A newer class of information-centric partnerships serves as a focal point for public and private entities to exchange insights and data to address national issues such as cybersecurity. These information-centric partnerships enable the government to harness private sector capabilities, efficiencies, and innovations for the public good, while also enabling attractive market forces useful for private enterprise. Data- and

[1] Of course, there are impressive cooperative efforts that are being undertaken. The work, for example, being done by the National Institute of Standards & Technology to create and implement security regimes stands out. So too do programs being managed by the Departments of Defense, Homeland Security (particularly significant recent guidance provided by the Cybersecurity and Infrastructure Security Agency) , and Health & Human Services. While necessary, these programs are not necessarily sufficient to deal with the pervasive cybersecurity risk that we are all facing. Thus, we offer a partial inventory of the resources currently available and suggest how critical cybersecurity information and talent might be shared to a greater extent in the present and future.

information-sharing partnerships in cybersecurity are often referred to as ISACs and ISAOs.

The topic of a government-endorsed ISAC was introduced in 1998 through Presidential Decision Directive No. 63 on Critical Infrastructure Protection (PDD-63), which advocated the establishment of private sector ISACs. PDD-63 also encouraged each critical infrastructure sector to establish sector-specific organizations (after consulting with, and receiving assistance from, the United States Government) for the purpose of "gathering, analyzing, appropriately sanitizing and disseminating private sector information" to its internal stakeholders and the National Infrastructure Protection Center.[2] The ISACs that were established in response have been designed to assist stakeholders in critical infrastructure sectors protect their physical and virtual assets from security threats in the real and electronic environments.[3]

ISAOs were created through a different vehicle, having been defined in the Homeland Security Act of 2002 (6 U.S.C. §131(5)) as "entities that gather, analyze, and share information on the security of critical infrastructure to assist in defense against and recovery from incidents." In February 2015, then-President Obama released Executive Order (EO) 13691, Promoting Private Sector Cybersecurity Information Sharing, which sought to improve information sharing for private sector entities via ISAOs. One of the reasons EO 13691 referenced ISAOs instead of ISACs, was that ISAOs are not limited to the critical infrastructure sectors.[4] Hence, an ISAC is an ISAO, but an ISAO is not necessarily an ISAC. The MITRE Corporation confirms that the wider aperture for ISAOs gives them:

> the potential to transform the landscape by complementing the current sector-specific sharing model represented by ISACs with a more flexible model that can support a highly distributed, highly diverse, and highly connected sharing ecosystem that is driven by the private sector.[5]

[2] Presidential Decision Directive (PDD-63), Critical Infrastructure Protection Annex A, May 28, 1998, available at https://fas.org/irp/offdocs/pdd/pdd-63.htm (last visited Oct. 6, 2018).

[3] National Council of ISACs, About ISACs, available at www.nationalisacs.org/about-isacs (last visited Oct. 6, 2018).

[4] Cybersecurity: Legislation, Hearings, and Executive Branch Documents, p. 2, Congressional Research Service, Oct. 21, 2016, available at www.everycrsreport.com/files/20161021_R43317_f0db220f9ad422bd1a91cc0255c73eeaa30e98fe.pdf; Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, Feb. 20, 2015, available at www.dhs.gov/sites/default/files/publications/2015-03714.pdf

[5] Bruce Bakis and Edward Wang, Building a National Cyber Information Sharing System, p. 9, MITRE Corporation (May 2017), available at www.mitre.org/sites/default/files/publications/building-national-cyber-information-sharing-ecosystem-pr-17-1125.pdf

This flexible model provides other advantages as well. ISAOs can be constructed as informal affinity groups or as chartered organizations resembling ISACs utilizing public-private partnerships. As a result, individual ISAOs can chose to focus their efforts within a geographic area, a functional group or industry sector, or on safeguarding specific events (sporting events and conventions).[6]

ISAOs were not intended to supplant or replace existing ISACs, but rather to lower the barrier for participation, thereby enabling small and medium-size businesses to engage in and benefit from the sharing effort. EO 13691 also intended for ISAOs to complement pre-existing ISACs by expanding information sharing practices within geographic regions, industry sectors, or to counter specific threats.[7]

4.2 DEFINITION

We define PPPs as a collaborative working relationship among industry, government, and others to take action toward a common mission through three shared elements:

- **Shared decision-making** – PPPs embody the principle of mutual self-determination and collaborative governance. The founding documents (e.g., charter, bylaws, legal agreements) explicitly codify how the partnership addresses questions such as who decides, how, and when. Unlike a traditional contractual arrangement in which one party specifies requirements to be delivered by another under the terms of a legal agreement, PPP partners generally retain the right to self-govern and operate autonomously yet collaboratively per their charter and agreements.

- **Shared resourcing** – PPPs involve pooled resourcing to achieve their mission. The resourcing, typically contributed by partners in a mutually agreed and fair manner, can take many forms. Contributions can include funding (via e.g., membership fees, subscriptions, product- or service-specific investments) and in-kind contributions (e.g., sharing data or information, volunteering time and expertise, offering tools and methods, and providing IT and other capabilities).

- **Shared benefit to partners and the public** – Successful PPPs deliver each partner a tangible return on their investment/contribution as well as a measurable public benefit. Given that participation in PPPs is voluntary,

[6] Ibid.

[7] Vincent Voci, Five Takeaways From the ISAO Conference, U.S. Chamber of Commerce, Feb. 18, 2016, available at www.uschamber.com/issue-brief/five-takeaways-the-isao-conference (last visited Oct. 27, 2018)

crafting a clear value proposition for each partner is critical to build and sustain the PPP. But this is not enough. The PPP must also be orchestrated to clearly demonstrate how the collaborative efforts of the partners through the PPP results in public benefit (e.g., safer world, economic growth, informed citizens). Adopting free enterprise principles (among other tenets of the Open Commons Framework[8]) brings market forces and innovation to bear in delivering these benefits.

Figure 4-1 illustrates these three elements of a PPP. Subsequent sections will unpack some of the real-world considerations that make this kind of partnership viable when applied to cybersecurity.

Figure 4-1: Elements of Private-Public Partnerships

5 CHARACTERIZING THE CHALLENGE

In this section, we explore how, despite government support and capacity building, challenges remain to all stakeholders due to the nature of collective cybersecurity risk.

In recent years, multiple entities within the federal government have called for greater private-public collaboration in the cybersecurity field. Indeed, PDD-63 and its resulting information sharing ecosystem demonstrates that at least as early as 1998 there was a strong belief in involving the private sector in collective measures.

National Security Presidential Directive 54 (NSPD 54) signed in 2008 called for a variety of cyber-related initiatives, including but not limited to: expanding cyber education; developing deterrence strategies and related programs; formulating a multi-pronged approach to address global supply chain risk management; and defining the Federal role to extend cybersecurity into critical infrastructure

[8] See https://www.cyberonmain.org/open-commons-framework/

domains. Presidential Policy Directive 41 (PPD-41), signed in July 2016, stated that individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

These calls for collaboration were expanded by the Cyberspace Solarium Commission's March 2020 report, which recognized that private-sector entities have primary responsibility for the defense and security of their networks. However, it is the U.S. government that is the sole entity who can bring to bear unique authorities, resources, and intelligence capabilities to support the private-sector actors with their defensive efforts. In light of this divide between private-sector responsibility and government capabilities, the Federal government

> must build and communicate a better understanding of the threats, with the specific aim of informing private-sector security operations, directing government operational efforts to counter malicious cyber activities, and ensuring better common situational awareness for collaborative action with the private sector.[9]

One of the recommendations that the Solarium Commission made is for Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (CISA) to strengthen a public-private, integrated cyber center within CISA to support its critical infrastructure security and resilience mission.[10] CISA is already designated as the lead federal department for the protection of critical infrastructure and has already developed and implemented numerous information sharing programs.

CISA's programs are intended to develop partnerships and share substantive information with the private sector, who are the owners and operators of the majority of the elements of the nation's critical infrastructure. CISA also shares information with state, local, tribal, and territorial governments (SLTT) and with international partners, as cybersecurity threat actors are not constrained by geographic boundaries.

CISA already has established the Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division to streamline strategic outreach to government and industry partners. SECIR strives to leverage capabilities, information, and intelligence, and subject matter experts to meet stakeholder requirements. SECIR programs build public, private, and international

[9] Cyberspace Solarium Commission Executive Summary, p. 6, United States Government, March 2020.
[10] Ibid., p. 7.

partnerships and capacity for resilience across the critical infrastructure and the cybersecurity community.

With so many thinktank calls and federal capabilities established, why, then, has it proven to be so vexing to achieve widespread adoption of information sharing[11] – and more importantly, what is the prescription for solving this predicament so that near-universal information sharing can be realized?

The following high-level topics serve as broad markers of challenges to be overcome to enable formation of collaboration structures that can foster widespread adoption of PPPs for collective cybersecurity. The remainder of this document builds upon these markers.

5.1 INSTITUTIONALIZING CYBERSECURITY AS COLLECTIVE RISK: CREATING A TRUST MODEL TO OVERCOME ENFORCEMENT CONCERNS

Because networks have been traditionally managed by the network owners, security has been institutionalized as an organizational problem. Moreover, sharing network-related details with outsiders has been anathema to the ethos of the IT professional. Indeed, the further sharing of sensitive data between government and industry represents an even deeper philosophical and cultural chasm. A “neighborhood watch” philosophy for the Internet has never been the dominant approach to security. Yet, sharing observations about community threats is central to the information sharing model. Accordingly, to change culture and behavior in ways that support private-public cybersecurity collaboration, leaders and professionals must embrace the notion that collective risk necessitates collective action.

To the extent that the positive culture we propose has not evolved on its own, we must examine the reason why the private sector has been resistant to more expansive information sharing. Indeed, it is not unfair to say that, while many private sector players have been happy to receive and act upon threat information from the government, they have been reluctant to provide information that might reveal or address vulnerabilities. Anticipating that such a problem might arise, Congress had enacted The Cybersecurity Information Sharing Act (“CISA law”), a United States federal law designed to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes".

[11] It is beyond the scope of this document to explore all the reasons, yet experience since PDD-63 suggests that factors such as the following are at play: knowledge gap, sector-based approaches prior to 2015, down-market appetite, business model gaps, and inadequate government support.

Indeed the CISA law provides substantial insulation from antitrust and other federal liability when threat vector information is shared with the government or among competitors. But the fundamental legal barrier has come from competing federal regimes like the Health Insurance Portability and Accountability Act, the enforcement of unfair competition law by the Federal Trade Commission, and the multiplicity of inconsistent State laws concerning data breach reporting and liability, and the security and privacy of personally-identifiable information. The State law picture has become even more muddled in the wake of the European Union's promulgation of the General Data Protection Regulation, which has served as a model for multiple new and enhanced U.S. State laws, particularly the California Consumer Privacy Act, which allows for private rights of action even without provable economic damages. Other states have emphasized particular issues of concern such as that covered by the Illinois Biometric Information Privacy Act.

As American companies increasingly are facing governmental enforcement actions at both the federal and state levels and private rights of action, largely through lawyer-driven class actions, and consequential significant monetary judgments and settlements, they have proved reticent to expose vulnerabilities, including breaches and ransomware attacks. The establishment of a truly-effective trust model, one that recognizes the ultimate threat to national security that attacks on our critical infrastructure, health care delivery system, public utilities and electoral processes require some additional legal protections. Among these, Congress should consider a uniform breach response law that preempts the state law patchwork that currently exists. And both federal and state legislatures might consider creating a rebuttal presumption of due care and legal compliance in the defense of regulatory and enforcement lawsuits where the entity at issue has demonstrably conformed its practices to the guidelines issued by agencies such as the NIST and the "tool kits" provided by CISA.

5.2 BUSINESS MODEL DESIGN AROUND COLLECTIVE RISK

It is therefore not surprising that along with resistance to collective approaches, the idea of information sharing and forming collective risk partnerships was not brought forth with any business model in mind. Without a business model, the concept can only, at most, achieve ad hoc adoption. To promote adoption of a collective risk approach, must therefore approach it as a viable commercial construct, and to that end incorporate answers to the standard business question: 'what's in it for me?' ("WIIFM"). While clarifying the value proposition alone will not solve the business model issue, it is a central requirement to overcome to achieve commercial viability. The model also should encompass working for legislative reform to clarify and limit legal liability while, at the same time assuring compliance with necessary best practices.

5.3 TRUST-ENABLING COMPONENTS OF COLLECTIVE RISK BUSINESS MODELS

In answering WIIFM, the business model must also ensure trust – for no sharing will endure if the sharing parties do not trust one another. Moreover, WIIFM should not countenance the “greed is good” philosophy advocated by the fictional Gordon Gekko from the film *Wall Street*. Rather, WIIFM and trust are the two core components for the functional collective risk cybersecurity business model. Balancing these two factors is the essential challenge for designing an effective and sustainable collective risk cybersecurity construct.

5.4 FOCUS ON SMALL BUSINESS, SUPPLY CHAIN, AND COMMUNITY

Trust is commonly an attribute or outcome of the local dynamic. Similarly, small business is a common feature of a local community. People frequent businesses they trust. Community – both in the geographic and relational senses – comes together and functions well because of trusted relations. Local communities foster trust and small business. As such, local communities integrally possess the core elements of a successful collective risk cybersecurity enterprise. Moreover, since small businesses often thrive in local communities, instituting private-public cybersecurity enterprises in local communities stands a better chance of success than in long-distance, distributed communities.

5.5 A BUSINESS MODEL FRAMEWORK THAT BALANCES MARKET FORCES AND TRUST

Taken together, the foregoing challenges instruct that the business model needed to achieve a commercial grade solution requires a balance between trust features and market features. Without either, the model will fail. Yet, business models have commonly achieved similar balancing of parties’ interests, such as through the use of business rules, calling upon business ethics, and enforcement through legal mechanisms.

6 BUSINESS CASE: THE BENEFITS OF PRIVATE-PUBLIC COLLABORATION

In this section, we illuminate potential benefits of PPPs for cyber information sharing to mitigate collective risk.

Many parties have stressed the need to align government and private-sector cybersecurity efforts. Information-sharing partnerships have delivered benefits in the healthcare, financial, transportation, and other sectors, as well as domains such as safety, innovation, and cybersecurity. Well-designed PPPs ensure that benefits accrue to all partners and to the public. Example benefits from PPPs are summarized below; note that some benefits may apply to both partners and the public. PPPs can:

- **Address complex problems beyond any one entity's reach.** This is both the primary driver for PPPs and the benefit that can happen at a macro level, across sectors and localities. Stated simply, some problems know no boundaries and cannot be solved or mitigated by any one entity. Recent studies have suggested that, because of low salary ceilings, governmental entities are in a competitively weaker position than private companies when it comes to hiring cybersecurity professionals. And, while the private sector might be relatively advantaged with respect to recruitment and in its knowledge base related to privately developed systems, governmental entities, especially those related to the Intelligence Community, the military and development agencies like DARPA, have unmatched expertise in certain areas that could benefit private entities, particularly those within the critical infrastructure. Properly formed PPPs harness the best attributes of both government and industry. By drawing on each partner's relative strengths in a way that complements other partners' relative weaknesses, the resulting capability is greater than the sum of the parts. Whether advanced cyber threats or other national challenges, the promise and challenge of a PPP is coming together to solve together what cannot be solved separately.

- **Foster economic growth.** PPPs, when fashioned in a community in pursuit of mutual interests, create new markets. Other PPP models also support growth in other ways. Partners' co-investment and shared resourcing itself is an indicator of potential and those efforts and contributions in and of themselves contribute to the economy. Moreover, PPPs frequently deliver outputs that lead to partners' growth in existing markets and/or identification of new markets and opportunities. Whether finding efficiencies, reducing risk, increasing effectiveness, or innovating solutions, the outcome of successful PPPs is often a more robust economy and opportunity space.

- **Leverage the power of co-investment.** By pooling resources to accomplish a shared mission together, each individual partner may only need to invest/contribute a small part of what they would have otherwise had to if they had funded the whole undertaking themselves. In addition, the nature of each partner's in-kind contributions can create a powerful synergy, for example by tapping into government's authority and intelligence and industry's innovation and market forces. Further, by contributing, they recognize a substantial benefit that reflects the scale of the partnership.

- **Deliver powerful insights from their unique vantage point.** Through the sharing and analysis of data that reflects a breadth of experiences and points of interest, PPPs by definition provide a broader view and often can detect signals in that shared data that would not be obvious in smaller or partner-specific datasets. From aggregation of data comes data-driven knowledge!
- **Enable partners to take meaningful action.** This bias toward action is a hallmark of well-designed PPPs. The shared capabilities in a PPP enables identification of common entities/actors, schemes, patterns, etc. that are of particular value to partners because they can take tangible action on those PPP-generated insights and, in so doing, also benefit the public interest. By focusing PPP operations on generating findings that are by design actionable, real progress happens each day.
- **Advance government's public service mission.** PPPs can help government realize the power of industry, academia, and others to advance its mission to serve Americans. By bringing the best that each partner has to offer, empowering PPPs enables government to be smarter and faster in responding to changes such as addressing a new problem, delivering some essential service, or responding to evolving expectations among its constituents about how government should function and to what end. Moreover, empowering PPPs may entail delivery of government-desired public services for which the government itself is not well-suited to deliver at the scale or in the manner desired.
- **Improve partners' internal efficiency.** By providing a shared capability set, partners can realize efficiencies in their own internal operations based on adopting – in whole or part – the methods, tools, lessons learned, and insights from the PPP. The beneficial effect on their internal operations due to exposure to a diversity of experiences and ideas is frequently called out as a benefit of participation in a PPP.
- **Drive innovation.** By engaging the brightest minds from academia, think tanks, industry, and other organizations, PPPs create a capability that fosters discovery, experimentation, and innovation. Cooperative research and development (R&D) agreements, joint R&D ventures, government-sponsored corporations, and other examples illustrate the power of partnerships being an engine for innovation and impactful R&D. Moreover, in a market-making construct, creation of new markets tends to drive new innovation.

- **Draw on the wisdom of crowds and networks.** The power of social networks, crowdsourcing, and collaboration has been established in literature and practice. Partners can realize substantial benefit from the emergent wisdom and insights that come from the collaboration and diverse perspectives common to many PPPs.

- **Enhance partners' effectiveness.** Many PPPs provide partners advance warnings of specific issues, insights into emergent trends, and/or some prioritization of concerns and related solutions. By leveraging these PPP-derived insights as a kind of triaging or focusing function, partners can focus their own operations on areas of highest return given limited resources. In terms of partners' mission effectiveness, PPPs can act as a force multiplier.

- **Accelerate time to impact.** While a single organization may take a certain time to realize the benefit of their internal processes, partners can get a boost by inheriting new insights and capabilities from the PPP faster than they may have been able to develop them on their own. Further, the nature of data-sharing partnerships means that as soon as the PPP identifies something from one partner, all partners are notified, often drastically reducing everyone's time to discovery, action, or impact.

- **Deter threat actors.** The Solarium Commission considers collaboration with the private sector to be one of the six pillars of a cyberspace deterrence strategy, and views PPPs in cyberspace as a desired end state that facilitates deterrence. Currently, the private sector owns the vast majority of critical infrastructure in the United States, which can result in planning and response efforts that are uncoordinated and ineffective; PPPs are a tool to align US interests in our nation's security with the private sector's interests through collaborative threat deterrence.

- **Motivate optimism.** The simple yet powerful realization that one is not alone – that others face the same problem and are willing to help – can be powerful in overcoming the sense of being overwhelmed, alone, or paralyzed by not knowing where to start. By signaling that others share interests and support/resources may be available, PPPs can serve to motivate that critical first step and quickly connect organizations together with capacity and community-based support. Government has been building this kind of capacity through ISAO SO and others.

- **Foster trust.** PPP members should meet periodically, in person or digitally, outside of contingent exchanges with regard to actual or perceived threats or operational issues. They can directly, or through committees, review best practices, describe compliance regimes, carry out "table top" exercises to test resilience, etc., and most of all establish and maintain the personal relationships that are key to establishing trust, not just in the abstract, but in the functional sense of promoting problem identification and solution in a cooperative manner, rather than in an enforcement mode.

As prospective partners shape the nature of their partnership, answering the question of what's in it for me (WIIFM) and how does a PPP provide greater benefit to all is critical. The list above can serve as a starting point for those discussions and way to more easily see how an organization's interests can align with – and derive benefit from participation in – a mutually-designed PPP.

7 A FRAMEWORK FOR ESTABLISHING A PRIVATE-PUBLIC PARTNERSHIP

In this section, we propose a framework for partners to use in co-creating a collective cybersecurity risk mitigation PPP that will deliver the kinds of benefits noted above.[12]

To realize the desired outcome of a more secure world, private sector entities need to engage with each other and with government under a shared governance model that promotes trust and innovation. As private and public organizations begin to work together in partnership to address cybersecurity challenges, they can benefit from designing their collaboration around three elements: interest, agreement, and capability, as illustrated in Figure 7-1.

[12] This section contains PPP framework content © 2020 The MITRE Corporation made available under a Creative Commons Attribution 4.0 International License: https://creativecommons.org/licenses/by/4.0/

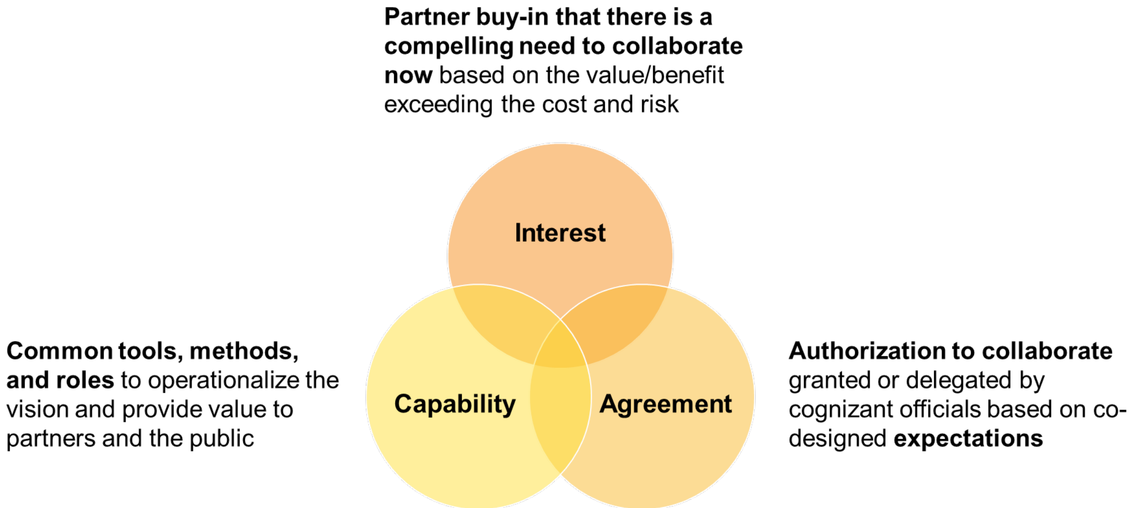

Figure 7-1. Three Success Drivers for Data-sharing PPPs

7.1 INTEREST

Partners – that is, the entities participating in the PPP – are initially brought together through the recognition that they face acute problems beyond the reach of any single partner to solve on its own. This galvanizing, shared interest is not just salient to each partner but is a compelling motivator to take action together. This leap of faith to work collaboratively – sometimes with competitors, regulators, or organizations with vastly different purposes and methods of achieving them – is the basis for PPPs.

Whether partners come together organically or are facilitated for example by a Trusted Third Party through a process that clarifies why they should participate, that initial rationale or justification for partnership is a necessary motivator for all that comes next. It can be helpful to consider how the path to realize the desired collaborative working relationship a journey of discovery and co-creation. To the extent it helps partners to understand what to expect early in the journey, we unpack how some PPPs can mature in the next section.

7.2 PPP DEVELOPMENT

PPPs often follow stages like those described in Table 7-1 below. Note that these stages are not necessarily linear or strictly contained. Not only might a PPP embody elements of multiple stages (e.g., circle back to ideate when faced with need to define its next phase of success, decide to pilot some new offering), but individual partners may be at different stages in their own level of participation.

Table 7-1. Common Stages in PPP Development

	Ideating	Planning	Piloting	Operating
Objective	Define a galvanizing mission and value proposition for establishing the partnership.	Recruit partners, build trust, and collaboratively develop plans for execution.	Demonstrate the value proposition (early wins) by starting small. Build trust. Build momentum, and rapidly learn what works for the partnership.	Transition to full operating capability. Expand the partnership to achieve greater impact.
Outcome	Funders and champions are committed to testing out the concept with a pilot.	Minimum set of partners have agreed to a working set of guiding principles, governance model, and plan of action for the pilot.	Initial operating capability. If successful, then may receive longer-term funding and commitment from partners to continue.	PPP is self-sustaining. Unique collaborative problem-solving capacity to address complex, wicked problems and achieve goals.

7.2.1 IDEATING STAGE

This stage is in many ways about capturing partners' interest and turning it into early forms of collaborative definition and action. In the ideating stage of a PPP, identifying what brings partners together is as essential as how they discover and clarify their shared mission. The facilitated discussions, negotiations, exploration of options, as well as writing and revising chartering documents together are all examples of early collaboration. By ensuring a collaborative approach to forming the PPP, the seeds of trust are planted and the partners recognize how their organization's interests and equities can be met in the nascent PPP (as well as respected by other partners).

7.2.2 PLANNING STAGE

In the planning stage, partners collaboratively define the overall benefit the PPP is intended to deliver, along with community or locality-based outcomes, the value proposition to industry and/or specific partners, and alignment to government public service missions. Consideration of cost and risk alongside the expected benefits ensures that a balanced and realistic business case emerges from the collaborative co-design process. Partners also draft the plan for how the PPP will deliver benefits and how they will work together under that framework and associated agreements.

7.2.3 PILOTING STAGE

In the piloting stage, a critical mass of partners takes individual and collective action to execute the plan, typically in a manner that provides quick wins with relatively little exposure/risk or effort. Often, agreements are achieved and executed at this stage that allow partners to share some sensitive data. Shared protocol and specific actions, studies, projects, working groups etc. help to prove out the PPP value proposition through the services or products the PPP may offer to partners. By collaborating on the initial operating capability (IOC), the partners learn how to enable the PPP to deliver on its objectives. Often the focus in this phase favors effectiveness (e.g., value delivery) over efficiency (e.g., cost/effort), given much is discovered and refined from trying and doing what was previously only conceived or planned.

7.2.4 OPERATING STAGE

In the operating stage, an increasing number of partners can participate more robustly in realizing the benefits of their contributions to the PPP. Based on lessons learned from the IOC, the partners have refined and revised aspects of the PPP to foster both effectiveness in value delivery and efficiency in operations. Through a continuous improvement mindset and a willingness to adapt to emergent needs and challenges, as well as lessons learned from the IOC, partners can create a virtuous growth cycle where early success leads to additional opportunity and justifies further investment that leads to continued success of the PPP.

7.3 AGREEMENT

The shift from mere expression of interest – where organizations see alignment with their own interests in participating in a PPP – to actually participating in the PPP and executing on its vision is bridged by agreement. As noted above, through activities that often occur in the planning and piloting stages, partners will converge upon a shared understanding of the nature and potential of their collaboration: what it is intended to achieve, how success will be measured, who might be involved in what roles, what contributions might be expected, what products or services might be shared with partners, how decisions will be made, how will partners work together, what role, if any, should a trusted third party play, and how these and other relevant expectations and concerns should be addressed. If we consider agreement to define the process leading to sufficient resolution of the questions the partners see as salient, two topics emerge: (1) what, when, and how does the PPP codify expectations and (2) who approves these based on what authority.

7.3.1 CODIFYING EXPECTATIONS

An organization's ability to partner with other entities and share data is often influenced by business, legal, privacy, security, and IT functions. These functions may have advisory, gatekeeping/veto, or decision authority. The PPP business case can strengthen a partner's ability to navigate their own internal approvals and politics, and help reframe those challenges as finding a path to yes. As with other aspects of a PPP, successfully framing agreements to work together and share potentially sensitive or proprietary information, often rests as much on how this is addressed as it does on what is addressed.[13] Regarding how to manage equities, the broad framework or guiding principles partners agreed to earlier can help shape and constrain the agreement which involves both business stakeholders and forward-leaning legal experts in a series of discussions and multiparty negotiations. Regarding what equities may need to be addressed, common topics among the partners (internal to the PPP) may include:

- use and ownership of intellectual property
- rights in data
- data protection including security, privacy, and permitted use expectations as well as applicable laws
- conflicts of interest
- precluding unfair competitive advantage and antitrust/anti-competitive concerns
- liability and warranty including seeking and obtaining legislative incentives and protections such as a uniform national breach reporting law that preempts the heterogeneous current State law regimes, and provides for compliance safe harbors against prosecution or regulatory enforcement,

[13] This section (Agreements) is distinct from Governance (see below). Whereas this section and its associated parts describes the impetus and means by which sharing parties agree to form a sharing partnership, the Governance section describes important features for standing up and operating the entity or facility through which the parties collaborate.

perhaps through rebuttable presumptions based upon conformity with stated federal best practices such as NIST guidelines.

- managing external information exposure through freedom of information, legal discovery, and general risk management
- and other expectations that are PPP-specific.

The result of these multiparty negotiations is consensus on expectations and accountability—codified in agreements of some form. Different agreements may be appropriate at different stages of the PPP's maturity. For example, a non-disclosure agreement may address confidentiality during the initiating stage but the planning stage may trigger a need for some memorandum of agreement, cooperative agreement, charter, and/or data sharing agreement. During execution, expectations may be codified in procedures or an operating manual.[14]

7.3.2 DRAWING ON AUTHORITIES

Contributing to the ability of partners to act on their interests and enter into some agreement(s) is the support of formal authority. Federal and SLTT governments can draw on statutory and other authorities. Examples may include the Economy Act, Bayh-Dole Act, Federal Technology Transfer Act, and OMB guidance, as well as DARPA, NASA, HHS, and other agency policies and precedents.

At the Federal level, Executive Orders 13636 (2013) and 13800 (2017) direct DHS to identify critical infrastructure at the greatest risk of a cyber incident resulting in catastrophic effects at a regional or national level, and to identify the authorities and capabilities that could be employed to support cybersecurity risk management efforts. The other side of Federal authorities is to provision oversight instrumentalities to ensure that whole-of-society activities do not conflict or interfere with government efforts related to national security, critical infrastructure, or other systemic institutions.[15]

Legislation can also create or clarify authorities. If enacted, the amendments added to the Senate Armed Services Committee version of the 2021 National Defense Authorization Act could expand and improve the authorities and capabilities for private-public information sharing. The proposals include:

- Establishing an information sharing environment between the Pentagon and the defense industrial base

[14] See Section 7.3 below on the Open Commons Framework™ can be a guide for balancing the parties' interests in constructing an agreement.

[15] For example, the willingness to contribute in whole-of-society initiatives, even well-intended volunteer efforts, can have unintended, negative consequences when no government-provisioned structure exists to channel efforts.

- Establishing a forensic malware repository between CISA and the National Security Agency
- Establishing a new Bureau of Cyber Statistics at the Department of Commerce and a new Bureau of Cyberspace Security and Emerging Technology at the State Department
- Scheduling of biennial tabletop cybersecurity exercises (including threat vector and ransomware response) along with a resolution supporting the creation of a new select committee in the Senate to focus on cybersecurity

Related capabilities at the State level vary significantly. However, the National Governors Association (NGA) is currently running a recently announced pilot program to enhance cybersecurity in seven states: Colorado, Michigan, Mississippi, New York, Oregon, Pennsylvania, and Tennessee. The NGA planning workshops with those states have already begun, and the efforts hope to learn from and build on the initiatives already in place for other states. Examples of these initiatives included:

- Partnerships with Academic Cyber Security Centers of Excellence to improve cybersecurity awareness in Arkansas, Georgia, and Indiana
- Creation of a Civilian Cyber Corps in Louisiana, Michigan, Ohio, and Wisconsin
- Coordination with their State National Guard units by Indiana, New York, North Carolina, Virginia, and Washington
- Conducting state-wide tabletop exercises involving Federal, SLTT, and private sector stakeholders by individual states or multi-state regions
- Establishing and funding Cyber Support Centers and threat intelligence sharing platforms
- Funding grants and scholarships for cybersecurity training of private sector residents

Commercial and academic institutions may draw on, for example, their charter, bylaws, and policies and procedures to determine who is authorized to commit the organization by executing the agreement(s).

7.3.3 APPROVING AND RESOURCING

Given a business case that is co-developed, organizations can then turn to their own internal stakeholders to approve it and ensure the ability and resourcing to deliver on the PPP-related expectations is put in place. That the PPP is moving from concept to reality often drives the need to clarify expectations, particularly around decision making, data sharing, and resourcing.

Partners may voluntarily, as part of PPP agreements, or based on their decision to acquire some PPP-provided product or service, invest resources in the PPP. These contributions can include direct financial and in-kind resources. Examples of financial resourcing include PPP membership fees, dues, payments for specific products or services, and in some cases equity or ownership stakes in the PPP. Examples of in-kind resourcing include the labor and expertise that individual participants put towards supporting the PPP, contributions of ideas, and of data (these may also have some monetary or other value attached to them). Regardless of the particular mix of resourcing, some non-zero contribution is often expected for potential participants to be recognized as and reap the benefits of being a partner. They may also benefit from leveraging capabilities already existing in the PPP and/or from capacity that has already been built (e.g., through government or industry efforts to date to bolster resources for cybersecurity) and thus can be inherited by the PPP.

7.4 CAPABILITY

Shared protocol (i.e., methods and systems for how partners manage and do work together) are often dependent on partners' expectations, resourcing, and the specific goals and attributes of the PPP. This section includes potential topics and considerations for defining the capabilities that enable the collaboration – and recognizes that each PPP must ascertain what is optimal for its situation. Broadly, PPPs often require some degree of partner convergence on topics such as:

- What is the operational tempo and nature of work (i.e., Concept of Operations)
- How precisely partners will share information, collaborate, troubleshoot issues/address conflict
- Data-related expectations (as appropriate) such as general or specific standards for what data elements are provided by whom, when, in what form; how data is managed; how data-driven products are developed, quality controlled, and disseminated to the right partners/stakeholders
- What policies & procedures should the PPP operate under
- What are the key performance indicators/metrics and how should accountability work
- What should the right mix and right level of common tools and supporting processes (i.e., capabilities) should look like (see subsections below)

The methods and systems partners use to collaborate and execute the work of the PPP are specific to the PPP based on its goals, resourcing, and nature of the core work. It can be helpful to consider which capabilities apply at what stage or phase of work, such as over the analytic lifecycle in the example of a data sharing and analysis PPP. One example illustration of the set of capabilities that may support a data sharing and analysis PPP is shown in Figure 7-2.

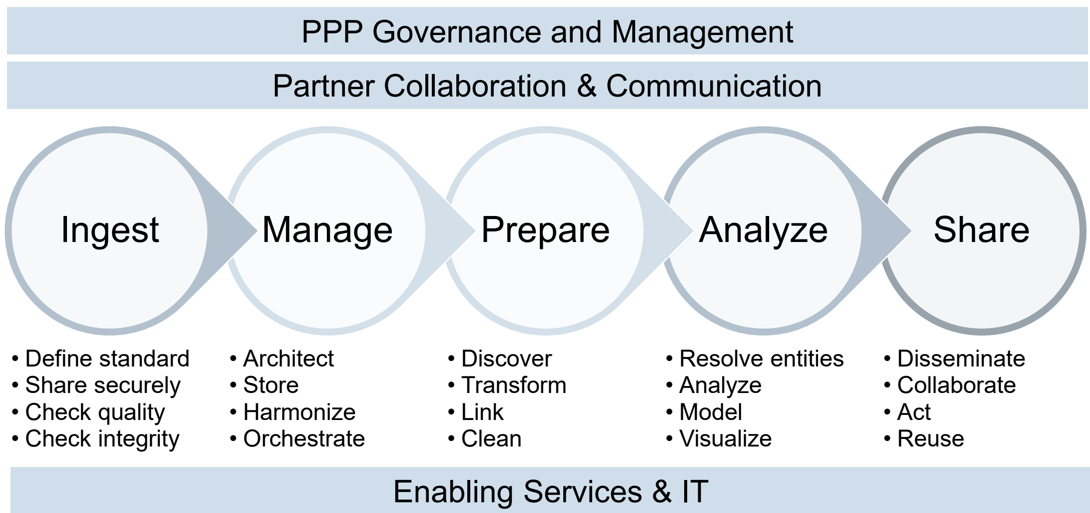

Figure 7-2: Illustration of Possible Protocol for Data Analysis PPP

While this illustration simplifies the activities and appears linear, in reality, PPPs with a data sharing and analysis focus can benefit from an iterative or agile approach. Regardless, PPPs can benefit from consideration of what systems and methods are optimal for the various workstreams or phases of the analytic lifecycle.

Broadly, PPPs often rely on an orchestrated suite of complementary capabilities to manage and execute on their mission. Below is a summary of 10 capabilities that can apply to PPPs. Whether, to what extent, and how, specific capabilities are required for the success of a given PPP varies and is highly situational. Therefore, this set of 10 capabilities is suggestive and should serve as a starting point for discussion and collaborative design among PPP stakeholders.

7.4.1 VALUE DELIVERY

Delivering benefit to partners and the public is the core reason for and success driver of a PPP. Value delivery applies people, processes, and technologies toward delivering PPP products and/or services (e.g., data sharing and analysis) that help the partners achieve their mission. This capability may also address fostering collaboration that is of value to the partners, providing the desired user experience, soliciting partner feedback on the PPP for continuous improvement, and measuring the performance and value of outputs and outcomes (to justify investment of time, talent, and funding).

The specific ways a PPP delivers value to its partners and the public is highly situational. For example, the value of a data sharing and analysis PPP rests on optimally designing and executing its data sharing, data storage and fusion, data analysis, and results validation and dissemination capabilities to produce actionable and measurably beneficial outputs for partners. PPP success is advanced when the value proposition – tangible products or services resulting in desired outcomes—is collaboratively defined by the partners. A Trusted Third Party can help facilitate and mediate this definition with the partners (and execute on that as desired by the PPP), especially if an independent and conflict-free view would mitigate partners' concerns about working directly with or sharing sensitive information with regulators, competitors, and/or unfamiliar entities.

7.4.2 OUTREACH AND COMMUNICATIONS

Outreach and Communications keeps the right partners engaged on the right topics in the right way at the right time. As such, this capability is central to the health of a PPP and tends to address: content authoring and delivery tools, collaboration tools, social media presence, campaign design and management (messaging, marketing), event management, and listening for the voice of the customer. Key activities may include understanding the stakeholder landscape, identifying early adopters, developing outreach materials, conducting introductory meetings and summits, communicating updates and information, and facilitating outreach and progress on necessary conversations e.g., to define the PPP concept.

7.4.3 INTAKE/SERVICE DESK

The Intake/Service Desk activates the methods and tools that support partner inquiries, requests, incident reporting, troubleshooting, and making suggestions/complaints. This capability may be informal or highly structured, lightweight or robust (multi-tier/multi-channel), concierge-style or semi-automated, all based on the specific needs of the PPP. It is often designed to address multiple topics (e.g., general, technical, procedural) pertinent to the specific PPP. Some concept of service levels and ticket management helps ensure responsiveness.

7.4.4 GOVERNANCE

Governance refers to the methods and systems used to direct and control the application of resources to advance the PPP's mission. Governance in a PPP is often focused on strategic decision-making (scope, priorities, funding, membership), sustainment, and providing input to operational management. The governance capability – sometime performed by a governance body or executive board – typically addresses roles, responsibilities, bylaws, and policies.

It can be helpful to differentiate governance from operational management of the PPP. Governance often addresses prioritization, strategy, resource allocation, policy formulation, and program/performance assessment – particularly as a topic's scope requires input from more than one organization or some form of group decision-making (e.g., consensus). Management often addresses optimization, operational focus, program execution, performance monitoring – in response to governance (e.g., direction from an executive board) – and is typically within a single person's span of control.

In a PPP, governance often explicitly addresses how shared decision-making works: who decides what, when, and how/by what method. Example considerations in a defining a typical PPP governance framework can include:

- Representation
- Voting and non-voting members
- Service terms
- Roles for members, chairpersons/co-chairs (and trusted third party, if applicable)
- Participation expectations
- Proxies
- Quorum
- Record keeping
- Foundational principles (e.g., transparency, reciprocity, fairness; see also §6, Operating Principles)

7.4.5 PROGRAM/OPERATIONS MANAGEMENT

Program/Operations Management orchestrates the regular, day-to-day activities of PPP staff (as applicable) and partners (to the extent they are contributing to core PPP efforts and activities). It is primarily concerned with product/service management, including the roadmap based on partner needs, and overall program management and integration (aligning efforts with expectations, given resourcing). This capability can:

- Provide clear insight into and management of the work queue and projects

- Ensure expectations for quality, scope, cost, and timeliness of delivery are met
- Respond to (governance-based) direction on prioritization by allocating available resources/capacity to that end
- Provide recommendations and tradeoffs to governance board (as applicable)

7.4.6 MEMBER MANAGEMENT

Member management helps PPPs productively and professionally to engage with a diverse, often numerous, set of partners. This can involve sufficiently robust tools and processes for managing the PPP membership, partners' varied expectations, and plans for and status of engagements with partners. It can also address how the PPP engages with other organizations, associations, and the government (e.g., if the government is not a full / voting member). Concepts and tools associated with Customer Relationship Management may be relevant in providing the necessary information (e.g., identity, roles, status, payments, participation) to effectively interact with current and prospective partners. This can be part of Outreach and Communications.

7.4.7 INNOVATION

Successful PPPs adapt effectively to emergent needs and environmental changes. This capability for innovation can support necessary advances in the PPP's offerings through, for example, a portfolio-based approach to effective business-driven investment in future capabilities, aligned research and development priorities, forecasting and visioning to shape path forward, and updating the PPP charter/products/services/business model to meet needs. It can also draw on partners' innovation capabilities, as made available to the PPP.

7.4.8 LEGAL AND COMPLIANCE

This capability provides legal support to the PPP in defining and managing its work to comply with relevant law and partner expectations. It can advise on managing partners' equities, provide counsel on legal obligations and compliance issues, draft standardized PPP agreements and structures to advance PPP mission, facilitate multiparty negotiations (e.g., on PPP agreements), inform business decisions based on expert assessment of legal risk, address conflict of interest and other concerns, and shape the codification of partner expectations for governance. It also provides a basis for liaison with legislative, regulatory and enforcement bodies to seek effective, cooperative solutions instead of reliance on litigation and formal process.

7.4.9 IT DELIVERY AND MANAGEMENT

To the extent that information-centric PPPs require a suite of supporting technical solutions, this capability can: elicit needs and identify solutions; make effective business-driven IT investments; forecast future needs; enable performant or on-demand IT solutions; provide responsive change management; efficiently operate and sustain IT; and deliver IT solutions (and related "-ilities" such as scalability) that meet PPP/partner expectations. This capability may also address how to optimally source the needed IT solutions and the role of partners in the PPP's technical ecosystem (e.g., users, solution providers).

7.4.10 SECURITY AND PRIVACY

Sustaining the trust partners place in the PPP and ensuring information is protected is paramount for PPPs. This capability addresses legal obligations and codified partner expectations for security and privacy controls (e.g., identity and access management, interconnection security, incident response, continuous monitoring) as part of a responsive approach to risk management supporting business goals.

8 OPERATING PRINCIPLES

When the stakeholders agree to form a structure to operationalize the services and features that have been agreed upon (e.g., through an ISAO or ISAC), the structure's governance provisions take on great importance. I In situations where the stakeholders charter an organization with growth ambitions (i.e., a local community's cyber and resilience entity possessed with an economic development mission), the governance mechanisms must carefully balance the trust and WIIFM aspects of the stakeholders in the business model. Special interests, or even unnecessarily protective, anti-competitive dynamics must be guarded against.

8.1 COMMERCIALIZING A SHARING ETHOS

The notion of "sharing" and "commercialization" might initially seem like a non sequitur. Yet, the openness of the Internet and the massive channel to market it facilitates has proven many times over that traditional proprietary and protectionist business approaches lose out to embracing openness, collaboration, and scale. As noted above, business rules can ensure that sharing parties align their interests in ways that promote growth.

With respect to ISAO or ISAC formation by the originating stakeholders, a useful reference for balancing sharing with growth is the open source software development community. Rather than tailored design of software, open source embraces crowdsourcing. While ownership (i.e., proprietary interests) should take a back seat to efficiency, nimbleness, and scalability, the adoption of open source also rests on the belief that the platform is often merely the conduit for sale of the product or service and facilitates the injection of inputs from a wider range of sources that might otherwise be filtered out by an organization that prioritizes ownership. More importantly and aside from the business strategy of open source software development principles, what's to be gained from open source is that its founders developed core tenets – known as the Open Source Definition. It represents a list of tenets upon which all open source development is supposed to adhere. It's a philosophical framework that embraces collaboration, openness, and efficiency.

Similar philosophical and governance tenets should promote information sharing and a collective approach to cybersecurity. Indeed, the Open Commons Framework™ was inspired by the open source community. However, rather than a methodology for software development, it provides a set of core tenets – or operating principles – to enable ISAOs and ISACs to meet the interests of their stakeholders and their users and partners. In this manner, the Open Commons Framework™ begins to institute a new ethos for information sharing in a manner that builds both trust and market forces.

8.2 CREATIVE COMMONS LICENSE STRUCTURE

Like open source software development, another institution triggered by the Internet revolution is the Creative Commons License[16]. In the context of a community cybersecurity initiative, a Creative Commons License provides a convenient way to foster collaboration and trust-building, while also enabling original and creative idea generators to receive credit for their works (albeit within the context of further sharing, derivatives, and improvements upon the original work through crowdsourced efforts). The Open Commons Framework™ (set out below) utilizes a Creative Commons License structure to promote further collaboration and development.

8.3 CORE TENETS OF THE OPEN COMMONS FRAMEWORK™

To facilitate the balance, described above, between building trust and promoting market forces to achieve commercial viability and scalability, the Open Commons Framework™ is outlined below as an option for operating principles.

1. **Free and Open Market Forces**

Adopters shall promote free enterprise principles and prohibit anti-competitive practices.

[16] See https://creativecommons.org/licenses/

Rationale: To enable market forces for economic vitality that promotes cyber resilience.

2. **Social Enterprise**

Adopters shall, in their articles of formation, specify that the entity's business purpose shall include the social objectives of improving a community's cyber resilience.

Rationale: To institute governance that promotes social enterprise within the market model.

3. **Enforceable Ethos**

Adopters shall hold themselves out publicly that in the entity's pursuit of its social objectives to its stakeholders, that it commits itself to the duties of loyalty, of fair dealing, and of care.

Rationale: To hold leaders accountable to the social enterprise.

4. **Innovation Protection**

Adopters shall institute governance by which original works and ideas are protected in ways that balance market forces and social enterprise principles.

Rationale: Social enterprise principles for collective cyber resilience should not undermine incentives that drive innovation.

5. **Trust Protection**

Adopters shall institute governance that balances collective interests with innovation principles.

Rationale: Innovators benefit for the trust established from a trusted partnership, and innovation incentives should not undermine trust that underpins the community.

6. **Main Street Friendly**

Adopters should institute "Main Street Friendly" business rules, policies and programs to advance economic vitality and innovation in the surrounding locality.

Rationale: Think Globally, Act Locally (in the context of building local cyber markets)

7. **Nurture Small Business**

Adopters should institute “Main Street Friendly” business rules, policies and programs that ensure that small businesses are not squeezed out of the local cyber market.

Rationale: About 50% of GDP and Employment comes from Small Business

8. **Creative Commons License – Attribution-NoDerivs (CC BY-ND)**

Adopters shall (if so designed by a local initiative), comply with the license terms indicated; and also should utilize a Creative Commons License for its own Main Street Friendly initiatives and original works.

Rationale: A sharing community that promotes Main Street Friendly ventures is simpatico with the Creative Commons construct, both philosophically and structurally

9. **Formation of Working Groups to Promote Derivatives**

Adopters that desire to advance derivatives and improvements of locally originated programs and original works in ways compliant with Creative Commons license restrictions (CC BY-ND) may do so through working groups formed by the local initiative founders. Similarly, adopters should pursue a similar working group model for their own Creative Commons licensed original works to advance derivatives and improvements.

Rationale: Improvements through derivatives are possible through collective efforts that still adhere to licensing terms

10. **Trademark and Open Commons Balance**

Adopters may be required to use the program mark in connection with any licensed use of founders’ local initiative.

Rationale: Consistency with license terms for “Attribution” and protecting trust through respect for IP interests (see FOSSmarks[17])

9 A COMMUNITY MODEL

The public component of the PPP embodies the fact that the organizing parties – who are seeking improved resilience through information sharing and other cybersecurity programs – also envision involving public agencies in their collective risk mitigation initiative. There are a variety of reasons why the private sector sees benefits of involving government, such as enhancing public safety,

[17] See https://fossmarks.org/

economic development, sharing resources, and other reasons. Often, government partners can be local, county, or state agencies. Indeed, trust – which is so vital for successful partnerships, especially for information sharing – can be enhanced from local connections. The idea of “community” derives from the characteristics present in local communities: friendship, collaboration, respect, common interest, and of course: TRUST! Accordingly, the PPP, as a way of championing and adopting cyber resilience and capacity building, can be fostered, grown, and institutionalized as a new path forward by focusing on local communities. That is, local communities can achieve their economic growth and cybersecurity resilience objectives, and sector leaders of the cybersecurity market can promote information sharing and business development, by working together to establish community-based Cyber PPPs.

A Community Model for Cybersecurity, referred to here as “Community Cyber”, often has the following attributes:

- Local leaders, cyber sector experts, stakeholders, and service adopters, all sharing a unified vision and set of objectives
- Economic development as a basis for establishment
- Familiarity with the capabilities and gaps in the local community
- Connections to local leaders (government, industry, and academia) deemed important to creation and sustainment
- Philosophical motivations for helping the local community, and its associated values and traits:
    - Willingness to contribute volunteer time
    - Trust in each other’s mutual acceptance of opportunity costs
    - Informality and social interaction among participants

9.1 STARTING POINT: COMMUNITY CYBER

The ISAO 6000 – 1 Issuance, and the ideas, framework, and tools outlined herein, can perhaps be most readily instantiated in a local community. Indeed, the societal consequences and adaptations necessitated by the COVID-19 pandemic can usefully lead to the rollout of community ISAOs. Why? Distance working may be a new reality. Yet, working from home and connecting to the office, utilizing consumer-grade Internet connectivity infrastructure, and the increase of devices operating outside the corporate perimeter all exponentially expand the attack surface. Is it likely that homeowners will spend the money necessary to achieve business-level security? Probably not. Accordingly, the time is ripe for solutions that increase security while driving down cost. An ISAO in a community presents an ideal construct for improving security in an economically sound way, rather than expecting individual households to universally achieve a heightened level of security.

Perhaps the best business case for establishing a Community Cyber initiative is to view community affinity outcomes as a competitive advantage. Associating with a pro-security initiative that elevates collective security creates advantages for its membership, especially if properly branded and marketed. Moreover, community-based initiatives have the inherent advantage of “community”. That is to say, there is a power to community that is absent from distributed and non-relational models. People and organizations are willing to support community initiatives in ways materially different than other commitments in that there is often a sense of duty and connection to that which is local and tangible.

9.2 MAIN STREET FRIENDLY MARKET FORCES

Listing Main Street Friendly among the core tenets of The Open Commons Framework™, signals the support of an idea that transcends an organizing philosophy. Main Street Friendly cyber PPP formation (i.e., a community ISAO) represents the embrace of localized economic development and the advancement of small business. Hence, the notion of instantiating ISAOs within communities because they are ideal environments for ISAO commercialization is strongly aided by the philosophical approach of The Open Commons Framework™. The dual interests of advancing ISAO creation and economic development converge and create additional synergies by promoting ISAO formation in communities.

10 FINAL THOUGHTS AND PATH FORWARD

The increasingly-daunting challenge of a establishing and sustaining a sufficient cybersecurity posture with limited resources need not be overwhelming – this Issuance shows that many organizations have not only discovered that they aren’t in this alone, but have already achieved some success through the frameworks and methods noted above for enabling PPPs for cyber information sharing. How might your organization partner with others to realize the many benefits of PPPs for cyber information sharing in your community?

11 APPENDIX A - REPRESENTATIVE PRIVATE SECTOR CONSTRUCTS AND ACTIVITIES

11.1 ISAO SO MARKETPLACE

The ISAO SO Marketplace is a one-stop shop for information sharing organizations to discover solutions such as services, tools, and capabilities which can assist them in growing their organization. The Marketplace offers a centralized collection of products, services and capabilities designed to assist ISAOs as they establish operations, meet the needs of their membership, and mature into successful information sharing organizations. Additional information is available at: https://www.isao.org/resources/marketplace/

11.2 C-MARKET

c-Market™ is a Community Marketplace for Cybersecurity Products and Services. The c-Market™ delivers cyber marketplace efficiencies to communities which drive down costs, make solutions more available, and open new community markets to vendors. The Community Cyber Market-Making Model is how market forces get generated at local levels. The result of making the local cyber market is a disruptive business approach that will return innovation, opportunity, and money-making to Main Street USA. Additional information is available at: https://c-market.us/site/

11.3 CYBERUSA

CYBERUSA is a national ISAO and collaboration of states focused on a common mission of enabling innovation, education, workforce development, enhanced cyber readiness and resilience. CYBERUSA provides a connective platform for locally structured and market-based ISAO activity as well as national resources for collaboration in economic development and innovation. CyberUSA is a ‘community of communities’, providing a funding methodology to support local efforts, while also providing exponential improvements to cyber resilience capabilities locally and nationally. Additional information is available at: https://www.cyberusa.us

11.4 MITRE

MITRE is a not-for-profit organization which works in the public interest across federal, state and local governments, as well as industry and academia. MITRE brings innovative ideas into existence in multiple areas to include cyber threat sharing, and cyber resilience. MITRE operates the National Cybersecurity FFRDC—sponsored by the National Institute of Standards and Technology—to help organizations address their most pressing cybersecurity needs. Additional information is available at: https://www.mitre.org/centers/national-cybersecurity-ffrdc/who-we-are

12 APPENDIX B - GLOSSARY

Selected terms used in the publication are defined below.

Actor: See threat actor.

Analysis: a detailed examination of data to identify malicious activity and an assessment of the identified malicious activity to existing threat information to say something greater about the data at hand.[18]

Attack: attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.[19]

Authentication: provision of assurance that a claimed characteristic of an entity is correct.[20]

Automated cybersecurity information sharing: the exchange of data-related risks and practices relevant to increasing the security of an information system utilizing primarily machine programmed methods for receipt, analysis, dissemination, and integration.[21]

Availability: property of being accessible and usable on demand by an authorized entity.[22]

Center for Infrastructure Assurance and Security (CIAS): is developing the world's foremost center for multidisciplinary education and development of operational capabilities in the areas of infrastructure assurance and security. The CIAS is a part of The University of Texas at San Antonio (UTSA).

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.[23]

Control: measure that is modifying risk.[24]

Cyber threat indicator: information that is necessary to describe or identify—

[18] ISAO 100-1. (2016, October 14). *Introduction to Information Sharing.* Retrieved from ISAO Support Organization: https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pd

[19] ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en. Retrieved: October 30, 2019

[20] Ibid

[21] ISAO 100-1, 2016

[22] ISO/IEC 27000:2018(en)

[23] Ibid

[24] ISO/IEC 27000:2018(en)

malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

a method of defeating a security control or exploitation of a security vulnerability;

a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

malicious cyber command and control;

the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or

any combination thereof.[25]

Cyber Threat Information (CTI): information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against information technology or operational technology systems.[26]

Cybersecurity information sharing: the exchange of data-related risks and practices relevant to increasing the security of an information system.[27]

Event: occurrence or change of a particular set of circumstances.[28]

Incident response: an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.[29]

Incident: a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[30]

[25] ISAO 300-1. (2016, October 14). Introduction to Information Sharing. Retrieved January 23, 2019, from ISAO Standards Organization: https://www.isao.org/storage/2016/10/ISAO-300-1-Introduction-to-Information-Sharing-v1-01_Final.pdf

[26] Ibid

[27] ISAO 100-1, 2016

[28] ISO/IEC 27000:2018(en)

[29] ISAO 300-1

[30] ISAO 100-1

Indicator: a technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.[31]

Information security: preservation of confidentiality, integrity, and availability of information.[32]

Information Sharing and Analysis Organization (ISAO): an ISAO is any group of individuals or organizations established for purposes of collecting, analyzing and disseminating cyber or relevant information in order to prevent, detect, mitigate, and recover from risks, events or incidents against the confidentiality, integrity, availability and reliability of information and systems.[33]

Integrity: property of accuracy and completeness.[34]

Jurisdiction: The geographic area over which authority extends; legal authority; the authority to hear and determine causes of action.

Mitigation: the act of reducing the severity, seriousness, or painfulness of security vulnerability or exposure.[35]

Monitor: to acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.[36]

Multi-State ISAC: an organization whose mission is to improve the overall cyber security posture of state, local, tribal and territorial governments.

Policy: intentions and direction of an organization, as formally expressed by its top management.[37]

Process: set of interrelated or interacting activities which transforms inputs into outputs.[38]

Requirement: a need or expectation that is stated, generally implied or obligatory.[39]

Security control: the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.[40]

---

[31] NIST. (2016, October). Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. doi:http://dx.doi.org/10.6028/NIST.SP.800-150

[32] ISO/IEC 27000:2018(en)

[33] ISAO SO (nd)

[34] ISO/IEC 27000:2018(en)

[35] ISAO 300-1

[36] Ibid

[37] ISO/IEC 27000:2018(en)

[38] Ibid

[39] Ibid

[40] ISAO SO 300-1

Security vulnerability: any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.[41]

Sensitive information: information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.[42]

Stakeholders: a person, group, or organization that has interest or concern in an organization.

Threat actor: an individual or a group posing a threat.

Threat information: any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.[43]

Threat: any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.[44]

Training: NIST 800-84 defines training as “informing personnel of their roles and responsibilities within a particular IT plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the IT plan”.[45]

Vulnerability: a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.[46]

Working group: a committee or group appointed to study and report on a particular question and make recommendations based on its findings.

---

[41] Ibid

[42] NIST 800-151

[43] Ibid

[44] NIST 800-151

[45] NIST SP 800-84 – September 2006 - Tim Grance (NIST), Tamara Nolan (BAH), Kristin Burke (BAH), Rich Dudley (BAH), Gregory White (UTSA), Travis Good (UTSA) - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. - https://csrc.nist.gov/publications/detail/sp/800-84/final

[46] ISAO 300-1

13 APPENDIX C - ACRONYMS

CC BY-ND	Creative Commons License – Attribution-NoDerivs
CISA	Cybersecurity and Infrastructure Security Agency
CISA	Cybersecurity Information Sharing Act
COVID-19	2019 Novel Coronavirus
CTI	Cyber Threat Information
DARPA	Defense Advanced Research Projects Agency
EO	Executive Order
EU	European Union
FBI	Federal Bureau of Investigation
FOSS	Free and Open-Source Software
GDPR	General Data Protection Regulation
HHS	United States Department of Health & Human Services
IOC	Initial Operating Capability
IoT	Internet of Things
IP	Intellectual Property
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISAO SO	Information Sharing and Analysis Organization Standards Organization
ISO	International Standards Organization
IT	Information Technology
MITRE	Massachusetts Institute of Technology Research & Engineering
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASA	National Aeronautics and Space Administration
NCCIC	National Cybersecurity and Communications Integration Center
NGA	National Governors Association
NIST	National institute of Standards and Technology
NSPD	National Security Presidential Directive
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PPD	Presidential Decision Directive
PPP	Public-Private Partnerships & Private-Public Partnerships
R&D	Research and Development
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
SP	Special Publication
TTPs	Tools, Techniques, and Procedures

U.S.	United States
U.S.C	United States Code
WIIFM	What is in it for me