Response to NIST Request for Information Number: 220210-0045

Comment for "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management."

Establishing Information Systems for Critical Infrastructure and Supply Chains With Data Privacy and Effective Regulatory Policy for Accountable Risk Management and Transfer Solutions

Author: Truman Esmond
Chair, Technical Steering Committee, **openIDL – *a Linux Foundation Project***
VP Membership & Solutions, **AAIS*, the American Association of Insurance Services***

Executive Summary

These comments outline a way to extend the NIST Cybersecurity Framework to enable Data Privacy for organizations and systems risk-related data that support increasingly accountable compliance mechanisms. The solution creates both commercial opportunity as well as community risk prevention and mitigation policy structures as organizations are connected and successfully, collectively perform their critical business and security Core Functions of Identify, Protect, Detect, Respond and Recover for Critical Infrastructure and Supply Chain systems.

openIDL (open Insurance Data Link, https://openIDL.org) is an organization, technology framework and distributed data mechanism, collaboratively developed and maintained with Government regulators, response organizations, Insurers, technology and data providers as well as industry data stewards. openIDL technology establishes Data Privacy for Data Owners, and objective information quality for Regulators and other Information Consumers, through transparent operations assured through Distributed Ledger Technology. openIDL governance allows Government entities and industry participants to accelerate and streamline increasingly timely and accountable information systems than previously possible.

Incorporating this new paradigm, the NIST CyberSecurity Framework can recommend mandatory minimum data protocols for Critical Infrastructure/Supply Chain segments and providers. These Community Standards for data integrity, utility and privacy enable Insurance industry and Government participation in preparation, response and ongoing collaborative mechanisms accelerating successful implementation, maintenance and delivery of the critical infrastructure components and services.

"*External Data Strategies*" developed and deployed for each participating role collectively informs a "*Community Data Strategy*." Each organization participating in the success of the specific operation or broad system function, is objectively accountable to their role towards collective performance. How each Organization meets their informational obligations is practical and within their control to deliver to specific, transparent and changing expectations, that are ultimately accountable to enforceable policy that increasingly assure expected performance of Critical Infrastructure and Supply Chains.

Table of Contents

Comment

The Data and Policy Problem

The data and information resources available to policymakers today simply cannot move fast enough or be relied upon for accurate information to make increasingly important decisions. Regulatory policy as a result struggles to make a "rule" that cannot be enforced or reasonably implemented to meet increasingly critical and specific risks. The best evidence of this is that we cannot make critical infrastructure cyber security policy mandatory or accountable to success, not just in the event of failure. Insurance and regulatory policy for risk transfer helps assure the public these risks beyond the capacity of an individual or enterprise are managed, through public and regulatory policy and industry data streams.

In society and in increasing number of risk situations, we find our policymakers dining on shitty data, so we get shitty policy – the Garbage In-Garbage Out rule. A little vulgarity is proven to garner attention, apologies for any offended sensibilities.

Enterprises feel this pain, defending claims of "overreach" and onerous compliance obligations, as well as increased litigation and fraud, and individuals still lack insurance products for our autonomous vehicle or for infrastructure support in managing our individual ransomware risk.

Engaging Regulators and Risk Industry

Enabling risk transfer and participation brings tools and resources delivering consistent and defined value at each step of the supply chain process, including financial and operational risk support of system and data security, particularly important in risk resilience and preparation, as well as timely coordinated response. Each party in delivering the Core Functions can be assured of secure, accountable information transfer and that their own data is kept private, through delivery standards that can be mandated in policy that includes transparent, responsive governance and accountability mechanisms appropriate to the risk.

Open Information Data Link, openIDL

This fundamental distributed data and governance framework, openIDL, or the "open Information/Insurance Data Link" has been part of the Linux Foundation for just over a year. openIDL is a transparent, accountable, community-of-communities data network that creates true data privacy, with practical, near-term incentives and quantifiable value for each and every community, infrastructure provider and Government entity involved. One of the first and fundamental "open governance" platforms under the Linux Foundation, openIDL is available as both open-source technology and open-source governance organizations, templates and places to connect into the broader community.

Applying openIDL in Critical Infrastructure and Supply Chains

These definitions can and should start with existing expectations and standards within and among enterprises, including the CyberSecurity Framework standards, and extending into industry data streams across relationships and common/proprietary systems, with particular attention to those involving State or Federal Government regulatory policy and event response agencies.

Each organization leverages their existing trusted data infrastructure to securely report periodic information according to transparent quality rules and protocols specific to the informational and functional purposes of the Community. Participation is completely in the control of each participant, with performance expectations defined, transparent and objectively enforced.

Specific Comments

The following specific suggestions for pursuit by the NIST and working groups will enable the above features and benefits:

1. Draft an External Data Strategy for each Critical Infrastructure/Supply Chain Participant, stating purpose, objectives, and process events. Each Strategy documents the Participant's – including Regulators and Government's – core roles, data objects, critical facts and contextual data points in coordinated/dependent processes and existing Core Framework processes, considering integration of regulatory reporting responsibilities and objective performance metrics the Participant expects and expects to deliver to, and is shared with the Community.

2. Establish one or more Critical Infrastructure/Supply Chain (CI/SC) Community Framework definitions to extend the mappings of the NIST CSF to each Participant's External Data Strategy as applicable to the Community for practical implementation to existing data streams and processes specific to the infrastructure and risks. It is critical that the resulting Community Frameworks be empathetic to the stakeholders and communities involved, while being specific to clear strategic purpose. Accountability and transparency is introduced and expected to evolve within the Framework to better support the **CI/SC Community**, even if starting from the voluntary status quo.

3. Establish transparent Community Governance Organizations (CGOs) to manage and deploy Community Platform Solutions (CPSs) as networked technology for CI/SC Community Participants. A CPS is a practical playing field that enables different Participating Organizations, with different Roles at different times in different Communities and Processes, to participate in a purposeful, accountable Distributed Data Network.

4. Leverage Open Source, community-driven technology to integrate existing or novel data, software and/or hardware of participants. Distributed Ledger Technology (DLT) assures the performance of the system and the data privacy, quality and value considerations of each stakeholder, over time and consistent with the CI/SC Community and Participants purpose.

5. Define and establish one or more Interaction Link Patterns (aka "extraction" patterns) within and across trusted CI/SC Communities and Participant entities within CPSs to accelerate, improve and regulate operations of the information and physical CI/SC to better inform and enable the CyberSecurity Framework Core Functions supporting specific, systemic and catastrophic risks, including Cyber threats.

6. Consider openIDL as an open source community organization, governance pattern and technical platform for the fundamental connection to real-world experience and private data from the systems, enterprise, industry, and community through to regulatory bodies for collaborative, specific governance (CGO) and data solutions (CPS) for integrated and evolving CI/SC Communities.

7. Extend the value proposition closer to consumers, developers and operational activity within industry, enterprises and proprietary systems through published **openIDL Community-specific APIs and DevOps** packages. As an open-source community platform, openIDL may be a considered and extensible solution for communities, organizations, and public entities at each, any and every level of system operation and supply chain collaboration.

We at openIDL and AAIS look forward to participating in future discussions to help our collective resilience, efficiency and opportunity for both disaster avoidance and improved performance for the future. We would invite everyone interested in improving CyberSecurity

for our Supply Chain and Critical Infrastructure and the future of data in risk transfer mechanisms to learn more about openIDL and the organizations involved.

Thank you for your interest in this Comment.

Additional Resources and Information

Please contact openIDL, AAIS or the Author for more information and resources and specific reads, resources & how to apply openIDL and participate by Audience:

1. CyberSecurity Framework Professionals
2. Private Industry & Enterprise
    a. Industry Business Executive(s)
    b. Industry Enterprise IT/Data Professional
    c. Industry Compliance Professional
    d. Vendor/Service/Solution Provider to Industry
3. Government
    a. Regulatory Policy & Compliance (e.g. Dept of Insurance, Federal Bureaus, etc.)
    b. Operational/Response Agency (e.g. Field Agencies, DMV, CISA, _EMA/EMS)
    c. Legislators and Elected Officials
4. Individual Contributors, Students, Educators and Institutions
    a. Learn more about how to implement and maintain
    b. Stand up a “Hello World” sample environment
    c. Start a collaborative educational Project
5. Entrepreneurs, Innovators and Consortia
    a. Learn more and how to design and apply openIDL for innovative solutions and opportunities in your own community
    b. Learn more and how to connect your innovations and community to regulators and/or the risk industry

Definitions

Data Community – an ecosystem of participating organizations and operational systems of different roles in the delivery of a business result or performance of a system, through the transparent interaction of their private data to objective performance criteria. Members may be Data Owners, Information Consumers and/or part of the Community Governance Organization stewarding the data network for the business purpose.

Participant/Member Organization – an entity uniquely credentialed in the openIDL Data Network, operating an openIDL Member Node, and credentialed having a Role in at least one Data Community for operations.

External Data Strategy – a document outlining the Organization’s Role in the Data Community, specifying the data maintained, information required, objectives sought and process events that affect the role or roles it plays in the ecosystem serving the business process, Supply Chain or Critical Infrastructure.

Community Data Strategy – a document managed by the Community Governance Organization, compiling and reflecting the different Participant Organization's External Data Strategies by transparent and responding to the responsibilities and expectations of each Role in CI/SC Community and business processes, including operational success metrics and exception handling events, used to guide and manage the Community Platform Solution.

Community Governance Organization (CGO) – a transparent, formally chartered governance committee of Members representing the Participating Roles in the Data Community and charged with the ongoing performance of the Data Community to the Community Data Strategy and metrics.

Community Platform Solution (CPS) – a technology stack employed by Members in the Data Community to perform of their responsibilities in the system as a Data Owner, Information Consumer or Governance Role in the context of the Critical Infrastructure/Supply Chain system. The complete stack is very specific to the Organization, the key components are shared and enable an "Enterprise Blockchain" network.

Distributed Ledger Technology (DLT), or Blockchain – a technology allowing the deployment of a shared ledger, synchronized copies across all members, with cryptographic linking or "chaining" of ledger transactions, assuring the integrity of stored data "blocks". Different DLT networks deploy different Consensus Mechanisms to assure block creation and integrity across members and transactions.

Consensus Mechanisms – in DLT/Blockchain systems, the algorithms and mechanisms that allow for the creation of data across the network, as it may be coming in from different nodes, so the network can trust that the blocks created are good and should be added to the shared ledger. The process is called "Consensus" and the rules for permitting new blocks on the network vary, and are most significant in Public, as opposed to Enterprise, DLT/Blockchain networks.

Enterprise (vs Public) Distributed Ledger Technology (aka "DLT" or Blockchain) Networks – are different primarily in that the ability to participate in the network is determined by the enterprise that governs the network, and the Members participate according to those rules and on technologies that may or may not be transparent. It is important to note that Public and Enterprise DLT/Blockchain networks are able to connect and interoperate – as long as the context is clear and is permitted by the Enterprise network.

Public DLT/Blockchain network – participation is voluntary and open. Like Bitcoin, anyone with the necessary computing power on the Internet can access the technology and establish themselves on the network, and can even create multiple unrelated identities. The underlying DLT/Blockchain technology may or may not be transparently managed or governed in Public networks, and technology governance, particularly in the variety of "Wallet" tools is particularly challenged. Consensus Mechanisms in Public networks rely heavily on complex algorithms, encryption and intense computation to approve adding new blocks to the network, so as

performance and efficiency demands increase, as well as necessary controls for regulated communities, Public DLT/Blockchain networks struggle.

Distributed Data Network – a data architecture where the "raw data", the facts in a system, are kept in the control and stewardship of the entities where the data is generated and the performance of the data capture activity is validated through Smart Contracts in the DLT/Blockchain network. When information is required about the data in the network, the "query" or Interaction Pattern, is distributed to the data through a second Smart Contract, and only the results of the query – anonymized, aggregated and lightweight due to the specificity and timeliness of purpose – is returned across the network.

Data Owners – Member organizations who deploy a node of the Data Network and maintain Data that is assured of integrity to the Role and Data Strategies and permit interactions with their data within the Community.

Information Consumers – Member organizations who deploy "Interaction Patterns" to return useful information from the Data Owners in the Data Network. Results from each Data Owner node in the Interaction Pattern "instance" is summarized to an Analytics Node, deployed by the Information Consumer Role or a Community Governance Organization service for delivery to the Community or participating Roles in the process.

openIDL Technology – openIDL is based on Hyperledger Fabric, an enterprise Distributed Ledger Technology (DLT) or Blockchain technology, an open-source community software project under the Linux Foundation. The openIDL technology stack includes other software for APIs, User Interfaces and management controls, the core libraries for which are open source and ready for augmentation by the Community or extension into proprietary environments and solutions.

openIDL Interaction Pattern, aka "Extraction" or "Link" Pattern – is the query or function performed on each Data Owner's node, interacting with their data and using the technology stack present, that is managed by the DLT/Blockchain technology to assure that this dynamic element of the openIDL Smart Contract processes consistent with the expectations of the Data Owner and delivers to meet the Information Consumers' needs.

openIDL Governance – the openIDL Network of technology-enabled Community ecosystems is governed under the structure of the Linux Foundation to ensure objective, community-driven leadership and participation. The three key committees include the openIDL Governing Board, the Regulatory Reporting Steering Committee, and the Technical Steering Committee. There are additional Working Groups supporting Data Models, Architecture and a variety of Application projects formed by openIDL Members and constituencies.

Linux Foundation – the oldest and largest community software organization, starting with the most widely used operating system, Linux, adding and supporting dozens of software and governance projects, including openIDL, Hyperledger, NodeJS, Kubernetes and more familiar technologies used worldwide.

Reference Information

openIDL, the open Insurance/Information Data Link

openIDL is a **Linux Foundation** (https://www.linuxfoundation.org) project chartered in April 2021 by a cross-section of Insurance industry organizations, including State Regulators and Departments of Insurance, technology organizations, industry associations and several leading Insurers. **openIDL** is a Community-driven Technology Platform, Distributed Data Network and Governance Structure that meets the practicality, control and privacy needs of Data Owners and the timeliness and quality needs of Information Consumers. The **openIDL** paradigm creates new opportunities for innovative solutions, improved performance across Members and Communities.

openIDL Current Projects

In addition to this NIST Comment, the following projects and working groups are underway and actively seeking additional participation:

1. Insurance Regulatory Reporting – NAIC Annual/Periodic Statistical Reporting
2. North Dakota Uninsured Motorists Proof of Concept – identifying and closing the uninsured motorist gap in ND as a model for the U.S.
3. Mississippi Coastal Catastrophe Pilot – MS Dept of Insurance, MS Emergency Management Agency (MEMA), technology providers and insurers collaborate for new preparation, response and recovery solutions in catastrophe exposed areas.
4. Intellectual Property and Content/Contract Provenance & Origination – aligning with the C2PA, Project Origin and related initiatives for risk solutions in a variety of content applications.

Please visit openIDL.org and sign up to join a project or gather folks to create your own and address the challenges or opportunities facing your Community.

openIDL Resources

1. openIDL.org Website: https://www.openIDL.org
2. openIDL.org Wiki: https://wiki.openIDL.org
3. openIDL.org Mailing Lists/Event Signup: https://lists.openIDL.org
4. openIDL.org GitHub: https://github.com/openidl-org/openidl-main
5. openIDL.org Contact Information:
    a. Executive Director: Jeff Braswell – [redacted]
    b. Community Director: Sean Bohan – [redacted]

AAIS – the American Association of Insurance Services

AAIS (American Association of Insurance Services) is a 501(c)6 not-for-profit Membership Association of U.S. Insurers, licensed by States as an Advisory Organization to the Property and Casualty Insurance Industry, for the purposes of data reporting to Regulators and facilitating Insurance Product development and availability as well as underwriting and policy standards for property and liability risks.

AAIS website: https://www.AAISonline.com

About the Author: Truman Esmond

Truman approaches nearly 5 years in the design, development and implementation of openIDL, joining AAIS nearly 10 years ago from a consulting career in digital marketing, network applications and solution design and development for dozens of notable clients in as many industries. After graduating Colorado State University with a BA in Business, Truman founded and led an early and successful web application development firm working with clients and pioneering technologies developing modern experiences and networked solutions. Acquired in 2008 to a larger interactive agency, Truman continued in various leading roles in solutions for familiar national brands before joining AAIS in 2012.

As Vice President of Membership and Solutions at AAIS, Truman leads the Member Engagement team supporting relationships for over 300 Member Insurers and Partners, business development pipelines and digital experience for the community. On the Solutions side, Truman leads technology strategy and many of the teams supporting operational platforms of the organization, including product adoption and automation, machine learning, regulatory reporting, Enterprise Content and Master Data Management infrastructure.

Truman serves on the Board of openIDL and as Chair of the Technical Steering Committee for openIDL, assuring the technology stack meets the needs of the Members and Applications of openIDL, after leading the architecture and development of the technology at AAIS since it's inception in early 2018.

Truman remains in Colorado and attempts to maximize time in the mountains on slopes and in rivers, with his wife Susan, three now-adult kids and a fair stable of furred and scaled critters.

Read more and connect directly with Truman (please make an effort to establish humanity):

LinkedIn: [redacted]
Twitter: [redacted]
Email: [redacted]