MIT
POLITICAL SCIENCE

Policy Analytics for Cybersecurity of Cyber-Physical Systems

Compilation by

Nazli Choucri
Professor of Political Science

and

Jerome Anaya
Research assistant

This complication is a Report of the MIT Project on Policy analytics for Cybersecurity of Cyber-Physical Systems. Gaurav Agarwal [a.k.a. Gaurav], MIT alumnus, served as Lead researcher for the Proof-of-Concept case presented here.

October 2024

ABSTRACT

Mounting concerns about safety and security have resulted in an intricate ecosystem system of guidelines, compliance measures, directives and policy reports for cybersecurity of all critical infrastructure. The policy paradox is that the text form of policy documents is an impediment to the implementation of policies and directives and creates potentially powerful opportunity costs.

As a general practice, guidelines, directives and policy documents are presented in text form, page-by-page and word-by-word all supported by figures, diagrams and tables as needed. By definition text obscures properties of both policy and system-target in terms of dynamic relationships, feedback, “drill-down”, leads and lags, and so forth.

The challenge is to develop analytics for cybersecurity policy of cyber physical systems. We begin with constructing (a) a structured system model of the system, in order to (b) identify major policy-defined system-wide parameters, (c) situate system vulnerabilities, (d) map security requirements to security objectives, and (e) advance research on how system properties respond to diverse policy controls for security of cyber physical systems.

This Project addresses the hard problem of policy-governed secure collaboration related to cyber-physical security of critical infrastructure (focusing on a generic and fundamental feature, namely smart grid of electric power systems). The purpose is to (a) reduce, if not eliminate barriers to full understanding of policy text as transmitted by the source, (b) explore system-wide or targeted implications, (c) help contextualize generic directives for specific applications, and (d) facilitate contingency analysis, as needed.

This Compilation is based on the Quarterly Research Reports submitted by MIT to the Cyber-Physical Systems Organization of Vanderbilt University. The Compilation is the first of several Reports highlighting the research process and products of the MIT Project on Policy Analytics for Cybersecurity of Cyber-Physical Systems. Gaurav Agarwal [a.k.a. Gaurav], MIT alumnus, served as Lead Researcher for the Proof-of-Concept case presented here.

Key Words: Proof-of-concept, text-as-data, design structure matrix, metrics, network models, Cybersecurity Framework, C-I-A, security, privacy, security objectives and requirements, impact levels

Disclaimer: This Compilation relies extensively on the Quarterly Research Reports. Any errors of omission or commission can be traced to the sources of these submissions.

References: Listed sequentially within each section.

Contents

List of Figures

List of Tables

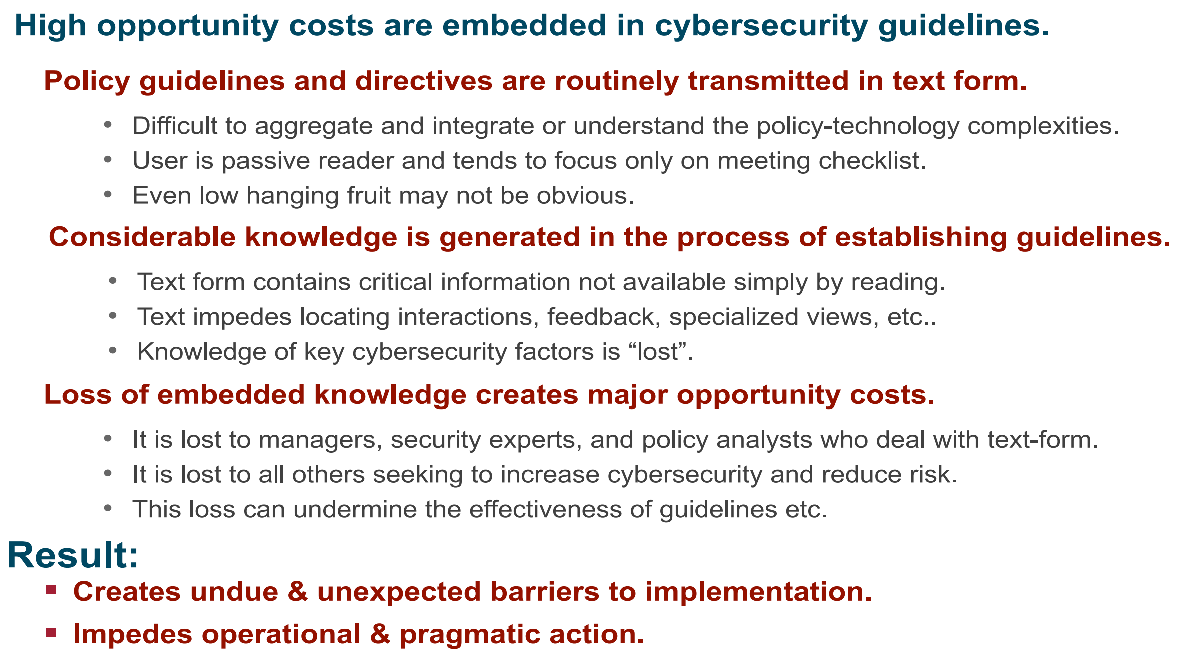
I. INTRODUCTION

Mounting concerns about safety and security have resulted in an intricate ecosystem system of guidelines, compliance measures, directives and policy reports for cybersecurity of all critical infrastructure. To date this has resulted in a complex ecosystem of policies that govern usage, data, compliance, security directives and the like for cyber-physical systems (CPS). The *policy paradox* is that the text form of policy is an *impediment* to the implementation of policies and directives and creates potentially powerful *opportunity costs*.

1.1. Problem Defined

By definition, guidelines and policies are written in linear sequential text form that makes them difficult to integrate, or to understand the policy-technology-security interactions, thus limiting their relevance for science of security. As a general practice, guidelines, directives and policy documents are presented in text form, page-by-page and word-by-word -- supported by figures, diagrams and tables as needed.

Rooted in the legal tradition, this practice reinforces a linear logic, where sequence dominates, and the focus is on compliance, step-by-step. Invariably this situation supports a checklist approach to meeting requirements. **Figure 1.1** summarizes the generic opportunity costs of text-based policy documents.



High opportunity costs are embedded in cybersecurity guidelines.

Policy guidelines and directives are routinely transmitted in text form.

- Difficult to aggregate and integrate or understand the policy-technology complexities.
- User is passive reader and tends to focus only on meeting checklist.
- Even low hanging fruit may not be obvious.

Considerable knowledge is generated in the process of establishing guidelines.

- Text form contains critical information not available simply by reading.
- Text impedes locating interactions, feedback, specialized views, etc..
- Knowledge of key cybersecurity factors is “lost”.

Loss of embedded knowledge creates major opportunity costs.

- It is lost to managers, security experts, and policy analysts who deal with text-form.
- It is lost to all others seeking to increase cybersecurity and reduce risk.
- This loss can undermine the effectiveness of guidelines etc.

Result:

- **Creates undue & unexpected barriers to implementation.**
- **Impedes operational & pragmatic action.**

Figure 1.1: The Underlying Problem

In addition, several *technical barriers* impede full understanding of the cyber-physical properties of a policy target. Such barriers include, for example, (a) locating policy relevant decision points, (b) identifying vulnerabilities embedded in organizational process and technical operations (c) Differentiating intents of threat actor vs. vulnerability of system, (d) tracking damages and diffusion effects, (e) characterizing potential unknown-unknowns, or (e) metricizing functional relationships – to note the most obvious.

Missing are analytics for cybersecurity policy and risk assessment. The challenge is to develop policy analytics for cybersecurity of cyber-physical systems (CPS).

1.2. Purpose

The *overarching* purpose of this Project is to support national strategy for cybersecurity, as outlined in the Presidential Executive Orders (EXORD) and the National Defense Authorization Acts (NDAAs). The goal is to develop analytics for cybersecurity policies and guidelines targeted specifically to (a) generate correctives for text-based policy features, (b) extract knowledge embedded in policy guidelines, and (c) assist the user community, analysts, and operators in policy implementation.

The Cybersecurity Framework (CSF) is mandatory in the public sector, and greatly encouraged for the private sector. CSF provides general guidance and directives of a broadly defined nature. But the mission-specific application is left to the user - with only general guidance provided by CSF. It is up to the user to proceed as best determined.

We situate this research project at the interface of user security concerns and CSF directives, in order to facilitate access to, and use, of CSF. The general purpose here is to help users and, in the process, provide tools to explore mission-related properties, concerns, or contingencies. For this reason, we have designed the entire project in modular terms to adapt to user needs.

1.3. Focus

Focusing on the salience of cybersecurity in both private and public sectors, we draw on major reports by the National Institute for Standards and Technology (NIST) as the source of our data. This material is rich in content, based on considerable background and collective knowledge, and subjected to careful scrutiny and evaluation.

While some efforts **[1, 2, 3 and 4]** have already been made to mine NIST materials, few exploit **[5, 6, 7 and 8]** the value of multi-methods for knowledge mining and analytical tools to support user understanding, analysis, and eventually action. References **[5-6]** visualize the information on the NIST smart grid conceptual model provided in reference **[9**]. Reference **[7]** examines the relationships or dependencies within the same conceptual model. Reference **[8]** provides a filtered view of the conceptual model for electric vehicles.

Put forth in details throughout this Report, our approach learns from, and transcends, the above by developing a platform for multi-methods cybersecurity analytics based entirely on the contents of policy documents. The case application, as *Proof-of-Concept*, focuses on cybersecurity of smart grid for electric power systems. The smart grid is a ubiquitous CPS, central to all critical infrastructures.

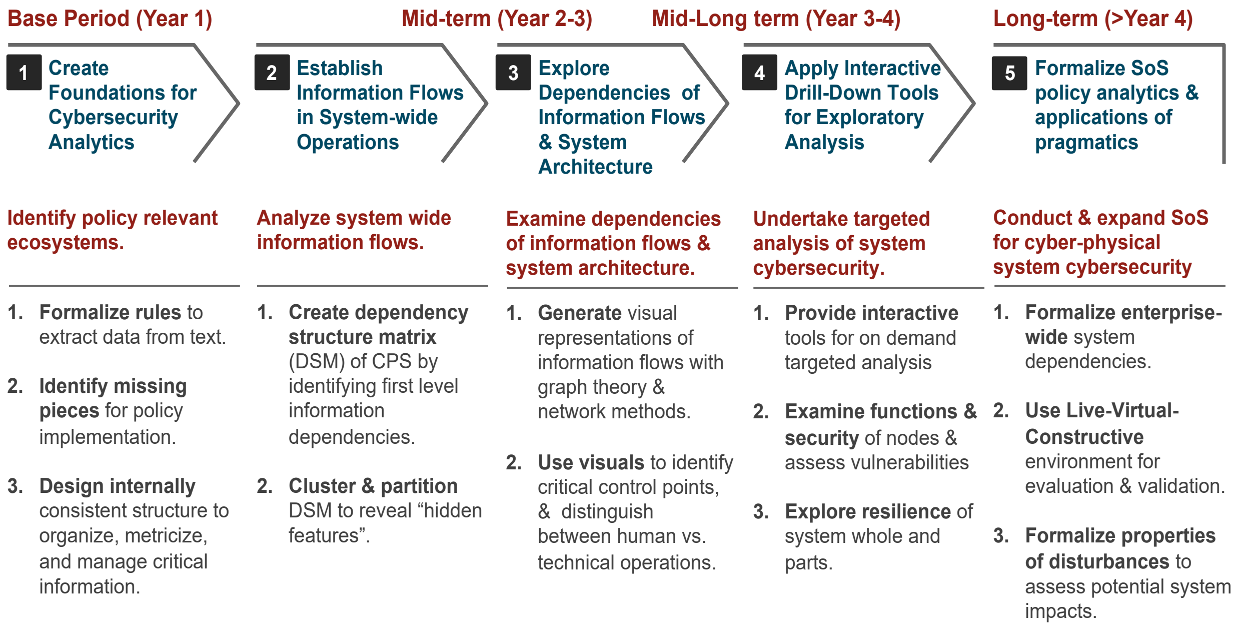
The *Proof-of-Concept* uses only policy documents as the database. As such, the case is in a "controlled environment". Further, the structured process developed in this Project (relevant to for any application) includes operational linkages to NIST-CSF to be set for mission-specific security requirements.

1.4. Method and Approach

As an introduction to the methods developed in this Project, we present a high level view of the major steps. The starting point is the policy text itself (or the cluster of policies that bear on the issues of interest). In modular terms, the steps are:

- Policy Text to Data
- Data to Framework
- Framework to Metrics
- Metrics to Model
- Model to Analytics for Policy

Figure 1.2 presents the near-, mid- and long- term project goals, focused on "Policy Governed Secure Collaboration" as the primary Hard Problem.



Base Period (Year 1)

1 Create Foundations for Cybersecurity Analytics

Identify policy relevant ecosystems.

1. **Formalize rules** to extract data from text.
2. **Identify missing pieces** for policy implementation.
3. **Design internally** consistent structure to organize, metricize, and manage critical information.

Mid-term (Year 2-3)

2 Establish Information Flows in System-wide Operations

Analyze system wide information flows.

1. **Create dependency structure matrix** (DSM) of CPS by identifying first level information dependencies.
2. **Cluster & partition** DSM to reveal "hidden features".

3 Explore Dependencies of Information Flows & System Architecture

Examine dependencies of information flows & system architecture.

1. **Generate** visual representations of information flows with graph theory & network methods.
2. **Use visuals** to identify critical control points, & distinguish between human vs. technical operations.

Mid-Long term (Year 3-4)

4 Apply Interactive Drill-Down Tools for Exploratory Analysis

Undertake targeted analysis of system cybersecurity.

1. **Provide interactive** tools for on demand targeted analysis
2. **Examine functions & security** of nodes & assess vulnerabilities
3. **Explore resilience** of system whole and parts.

Long-term (>Year 4)

5 Formalize SoS policy analytics & applications of pragmatics

Conduct & expand SoS for cyber-physical system cybersecurity

1. **Formalize enterprise-wide** system dependencies.
2. **Use Live-Virtual-Constructive** environment for evaluation & validation.
3. **Formalize properties of disturbances** to assess potential system impacts.

Figure 1.2: Near-, mid- and long- term project goals

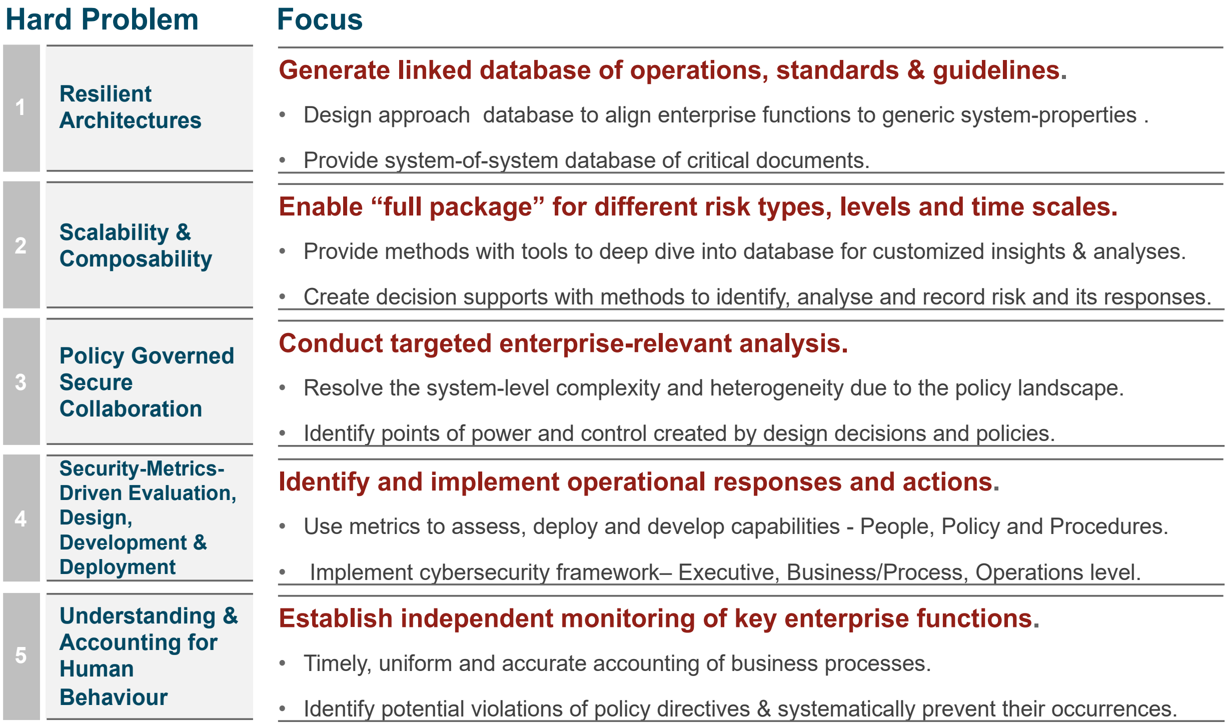
The research approach is based on structured analysis of critical policy texts designed to (a) identify major system-wide parameters, (b) situate vulnerabilities, (c) map security requirements to security objectives, (d) advance research on how multiple system features interact with multiple security requirements and affect the cybersecurity of critical cyber/physical enterprise, and (e) explore interactions of policy interventions and system-properties, including implications of "drill-down" investigations.

1.5. Contributions to Hard Problem(s)

As noted, this Project directly addresses the Hard Problem of Policy-Governed Secure Collaboration at the enterprise level (focusing on smart grid in electric power systems, as a class of cyber-physical systems central to the nation's critical infrastructure). The 2015 White Paper on the Science of Security Lablet defines the Policy-Governed Secure Collaboration as seeking to:

> "… develop the science underlying methods for expressing and enforcing normative requirements and policies for handling data with differing usage needs and among users in different authority domains." **[10]**

Figure 1.3 defines the Project contributions to the set of Hard Problems.



	Hard Problem	Focus
1	Resilient Architectures	**Generate linked database of operations, standards & guidelines.** • Design approach database to align enterprise functions to generic system-properties . • Provide system-of-system database of critical documents.
2	Scalability & Composability	**Enable "full package" for different risk types, levels and time scales.** • Provide methods with tools to deep dive into database for customized insights & analyses. • Create decision supports with methods to identify, analyse and record risk and its responses.
3	Policy Governed Secure Collaboration	**Conduct targeted enterprise-relevant analysis.** • Resolve the system-level complexity and heterogeneity due to the policy landscape. • Identify points of power and control created by design decisions and policies.
4	Security-Metrics-Driven Evaluation, Design, Development & Deployment	**Identify and implement operational responses and actions.** • Use metrics to assess, deploy and develop capabilities - People, Policy and Procedures. • Implement cybersecurity framework– Executive, Business/Process, Operations level.
5	Understanding & Accounting for Human Behaviour	**Establish independent monitoring of key enterprise functions.** • Timely, uniform and accurate accounting of business processes. • Identify potential violations of policy directives & systematically prevent their occurrences.

Figure 1.3: Addressing Hard Problems

We recognize that "Hard Problems" are particularly elusive because:

- Problem-properties are not discernable by traditional or well recognized modes of inquiry;
- Issue-area or domain has not been subject to extensive analysis to date;
- Temporality is not always reflected in even intervals;
- Data-creation is a necessary, but not sufficient, condition for progress; and
- System-boundary may not be easily defined, especially with overlapping systems.

In this context, **Figure 1.4** superimposes the relevance of the research design in this project shown in **Figure 1.3** onto the Hard Problems defined by the NSA Science of Security and Privacy Program.

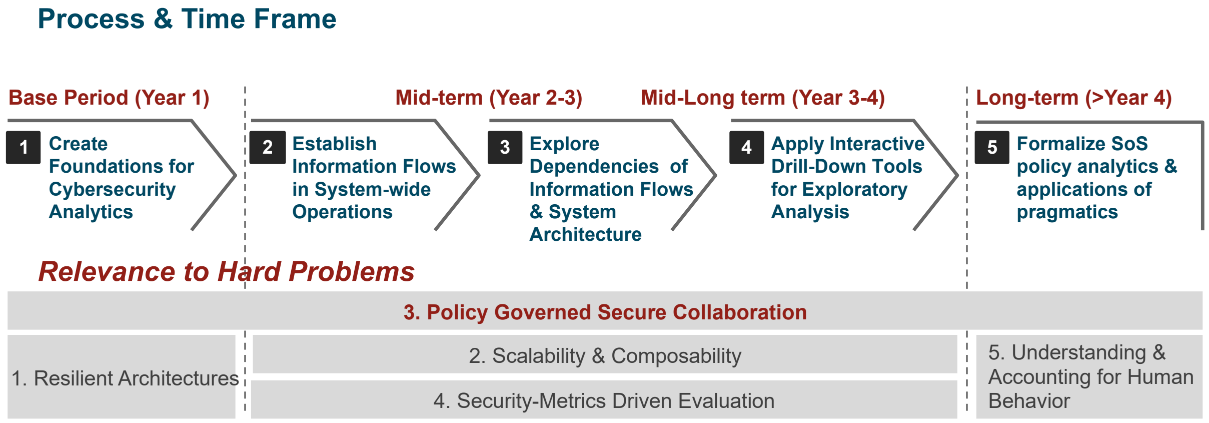

Process & Time Frame
Base Period (Year 1)
Mid-term (Year 2-3)
Mid-Long term (Year 3-4)
Long-term (>Year 4)
1 Create Foundations for Cybersecurity Analytics
2 Establish Information Flows in System-wide Operations
3 Explore Dependencies of Information Flows & System Architecture
4 Apply Interactive Drill-Down Tools for Exploratory Analysis
5 Formalize SoS policy analytics & applications of pragmatics
Relevance to Hard Problems
3. Policy Governed Secure Collaboration
1. Resilient Architectures
2. Scalability & Composability
4. Security-Metrics Driven Evaluation
5. Understanding & Accounting for Human Behavior

Figure 1.4: Situating Project Relevance to Hard Problems

The key point is this: while the focus is on Policy Governed Security Collaboration, our entire research design contributes to other Hard Problems as situated in **Figure 1.4**.

1.6. Expected Products

The research products of this Project include, but are not limited to:

(a) methods to examine the implications of cybersecurity directives and guidelines directly applicable to their system,

(b) information about relative vulnerability pathways throughout the whole or parts of system-network as delineated by the guidelines documents,

(c) insights from contingency investigations, that is, “what...if...”,

(d) framework information management within the organization, and

(e) ways to facilitate information flows bearing on decision-making for cybersecurity.

The following **Section** introduces the complex policy ecosystem governing cybersecurity in the United States, and provides a policy-centric context for this research initiative.

I. INTRODUCTION: References

1. Cyber Security Procurement Requirements Traceability for the Electric Sector, Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002003331, 2014. https://www.epri.com/#/pages/product/3002003255/

2. Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002003332, 2014. https://www.epri.com/#/pages/product/3002003332/

3. Risk Management in Practice, Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002003333, 2014. https://www.epri.com/#/pages/product/3002003333/

4. Cyber Security Risk Management in Practice, Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002004712, 2014. https://www.epri.com/#/pages/product/3002004712/

5. M. Harvey, D. Long and K. Reinhard, "Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security," 2014 Power and Energy Conference at Illinois (PECI), Champaign, IL, 2014, pp. 1-8. https://ieeexplore.ieee.org/document/6804566

6. D. Long, B. Drennan, and K. Reinhard, "NISTIR 7628 Visualization", Cyber Resilient Energy Delivery Consortium (cred-c.org). https://cred-c.org/sites/default/files/posters/19_SynchDataQ_Poster_CREDC%20IW%2017.pdf

7. B. Rogers and E. Gilbert, "Identifying architectural modularity in the smart grid: an application of design structure matrix methodology", Grid-Interop Forum, Phoenix AZ, 2011. https://sdm.mit.edu/news/news_articles/webinar_082012/rogers_082012.pdf

8. C. F. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," in IEEE Communications Magazine, vol. 51, no. 1, pp. 58-65, January 2013. https://ieeexplore.ieee.org/document/6400439

9. NIST, "Guidelines for Smart Grid Cybersecurity," NISTIR 7628, Revision 1. September 2014. https://doi.org/10.6028/NIST.IR.7628r1

10. Nicol, D., B. Sanders, J. Katz, B. Scherlis, T. Dumitraș, L. Williams, and M.P. Singh. 2015. Science of Security lablet: Progress on Hard Problems. p2. https://cps-vo.org/node/21590

II. COMPLEXITY of CYBERSECURITY POLICY

Section II focuses on the policy domain or ecosystem for this Project. The purpose is to situate the Project and its *Proof-of-Concept* in the vast cybersecurity policy landscape.

2.1. Dilemmas for Complexity of Policy Domain

The complexity of the policy-domain governing cybersecurity is evident 2018 when the Office of US Deputy CIO, Department of Defense released a landscape view of cybersecurity related policies This dense document refers to a set of at least 181 texts, aggregated into nine broad categories. One set is the NIST SP800 series documents which itself consists of over 195 documents.

Policy-domain complexity raises the following questions, among many:

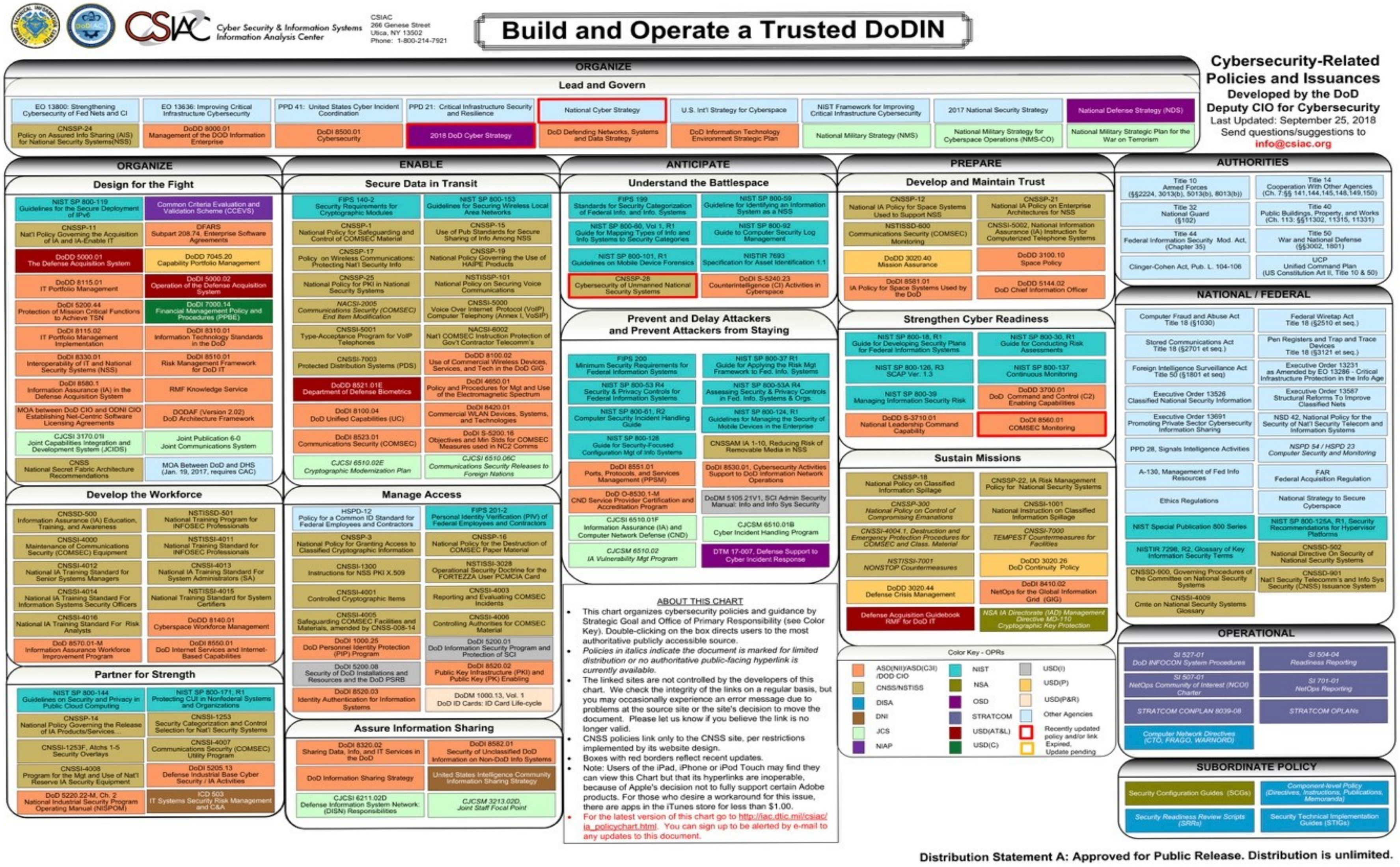
- How to locate the desired texts and cybersecurity specifications defined by specific circumstances?
- How to identify additional requirements or non-compliances if existing process, technology, or condition is changed?
- How can analysts extract the "full-logic" of cybersecurity policy-texts?

Given that cybersecurity directives are text based and run into hundreds of pages, how do we expect a policy analyst of war-fighter to navigate through this policy domain?

Then, too, how can we best leverage the current policy landscape to retrieve and examine the knowledge embedded in text and, as needed, capture its utility?

In the absence of an information sheet on *what* to refer, *when*, *where,* and by *whom,* the challenge still remains of determining actions, impacts, and consequences – over and above basic compliance measures.

Somewhat overwhelming is the summary of the cybersecurity policy domain provided by DoD in 2018, presented in **Figure 2.1** below. Is this vast policy landscape an impediment to effective cybersecurity? If so, how? If not, why not?



CSIAC
Cyber Security & Information Systems Information Analysis Center

CSIAC
266 Genese Street
Utica, NY 13502
Phone: 1-800-214-7921

Build and Operate a Trusted DoDIN

Cybersecurity-Related Policies and Issuances
Developed by the DoD Deputy CIO for Cybersecurity
Last Updated: September 25, 2018
Send questions/suggestions to
info@csiac.org

ORGANIZE

Lead and Govern

- EO 13800: Strengthening Cybersecurity of Fed Nets and CI
- EO 13636: Improving Critical Infrastructure Cybersecurity
- PPD 41: United States Cyber Incident Coordination
- PPD 21: Critical Infrastructure Security and Resilience
- National Cyber Strategy
- U.S. Int'l Strategy for Cyberspace
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- 2017 National Security Strategy
- National Defense Strategy (NDS)
- CNSSP-24 Policy on Assured Info Sharing (AIS) for National Security Systems(NSS)
- DoDD 8000.01 Management of the DOD Information Enterprise
- DoDI 8500.01 Cybersecurity
- 2018 DoD Cyber Strategy
- DoD Defending Networks, Systems and Data Strategy
- DoD Information Technology Environment Strategic Plan
- National Military Strategy (NMS)
- National Military Strategy for Cyberspace Operations (NMS-CO)
- National Military Strategic Plan for the War on Terrorism

ORGANIZE

Design for the Fight

- NIST SP 800-119 Guidelines for the Secure Deployment of IPv6
- Common Criteria Evaluation and Validation Scheme (CCEVS)
- CNSSP-11 Nat'l Policy Governing the Acquisition of IA and IA-Enable IT
- DFARS Subpart 208.74, Enterprise Software Agreements
- DoDD 5000.01 The Defense Acquisition System
- DoDD 7045.20 Capability Portfolio Management
- DoDD 8115.01 IT Portfolio Management
- DoDI 5000.02 Operation of the Defense Acquisition System
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve TSN
- DoDI 7000.14 Financial Management Policy and Procedures (PPBE)
- DoDI 8115.02 IT Portfolio Management Implementation
- DoDI 8310.01 Information Technology Standards in the DoD
- DoDI 8330.01 Interoperability of IT and National Security Systems (NSS)
- DoDI 8510.01 Risk Management Framework for DoD IT
- DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System
- RMF Knowledge Service
- MOA between DoD CIO and ODNI CIO Establishing Net-Centric Software Licensing Agreements
- DODAF (Version 2.02) DoD Architecture Framework
- CJCSI 3170.01I Joint Capabilities Integration and Development System (JCIDS)
- Joint Publication 6-0 Joint Communications System
- CNSS National Secret Fabric Architecture Recommendations
- MOA Between DoD and DHS (Jan. 19, 2017, requires CAC)

Develop the Workforce

- CNSSD-500 Information Assurance (IA) Education, Training, and Awareness
- NSTISSD-501 National Training Program for INFOSEC Professionals
- CNSSI-4000 Maintenance of Communications Security (COMSEC) Equipment
- NSTISSI-4011 National Training Standard for INFOSEC Professionals
- CNSSI-4012 National IA Training Standard for Senior Systems Managers
- CNSSI-4013 National IA Training Standard For System Administrators (SA)
- CNSSI-4014 National IA Training Standard For Information Systems Security Officers
- NSTISSI-4015 National Training Standard for System Certifiers
- CNSSI-4016 National IA Training Standard For Risk Analysts
- DoDD 8140.01 Cyberspace Workforce Management
- DoD 8570.01-M Information Assurance Workforce Improvement Program
- DoDI 8550.01 DoD Internet Services and Internet-Based Capabilities

Partner for Strength

- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-171, R1 Protecting CUI in Nonfederal Systems and Organizations
- CNSSP-14 National Policy Governing the Release of IA Products/Services...
- CNSSI-1253 Security Categorization and Control Selection for Nat'l Security Systems
- CNSSI-1253F, Atchs 1-5 Security Overlays
- CNSSI-4007 Communications Security (COMSEC) Utility Program
- CNSSI-4008 Program for the Mgt and Use of Nat'l Reserve IA Security Equipment
- DoDI 5205.13 Defense Industrial Base Cyber Security / IA Activities
- DoD 5220.22-M, Ch. 2 National Industrial Security Program Operating Manual (NISPOM)
- ICD 503 IT Systems Security Risk Management and C&A

ENABLE

Secure Data in Transit

- FIPS 140-2 Security Requirements for Cryptographic Modules
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material
- CNSSP-15 Use of Pub Standards for Secure Sharing of Info Among NSS
- CNSSP-17 Policy on Wireless Communications: Protecting Nat'l Security Info
- CNSSP-19 National Policy Governing the Use of HAIPE Products
- CNSSP-25 National Policy for PKI in National Security Systems
- NSTISSP-101 National Policy on Securing Voice Communications
- *NACSI-2005 Communications Security (COMSEC) End Item Modification*
- CNSSI-5000 Voice Over Internet Protocol (VoIP) Computer Telephony (Annex I, VoSIP)
- CNSSI-5001 Type-Acceptance Program for VoIP Telephones
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecomm's
- CNSSI-7003 Protected Distribution Systems (PDS)
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG
- DoDD 8521.01E Department of Defense Biometrics
- DoDI 4650.01 Policy and Procedures for Mgt and Use of the Electromagnetic Spectrum
- DoDI 8100.04 DoD Unified Capabilities (UC)
- DoDI 8420.01 Commercial WLAN Devices, Systems, and Technologies
- DoDI 8523.01 Communications Security (COMSEC)
- DoDI S-5200.16 Objectives and Min Stds for COMSEC Measures used in NC2 Comms
- *CJCSI 6510.02E Cryptographic Modernization Plan*
- *CJCSI 6510.06C Communications Security Releases to Foreign Nations*

Manage Access

- HSPD-12 Policy for a Common ID Standard for Federal Employees and Contractors
- FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors
- CNSSP-3 National Policy for Granting Access to Classified Cryptographic Information
- CNSSP-16 National Policy for the Destruction of COMSEC Paper Material
- CNSSI-1300 Instructions for NSS PKI X.509
- NSTISSI-3028 Operational Security Doctrine for the FORTEZZA User PCMCIA Card
- CNSSI-4001 Controlled Cryptographic Items
- CNSSI-4003 Reporting and Evaluating COMSEC Incidents
- CNSSI-4005 Safeguarding COMSEC Facilities and Materials, amended by CNSS-008-14
- CNSSI-4006 Controlling Authorities for COMSEC Material
- DoDI 1000.25 DoD Personnel Identity Protection (PIP) Program
- DoDI 5200.01 DoD Information Security Program and Protection of SCI
- DoDI 5200.08 Security of DoD Installations and Resources and the DoD PSRB
- DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoDI 8520.03 Identity Authentication for Information Systems
- DoDM 1000.13, Vol. 1 DoD ID Cards: ID Card Life-cycle

Assure Information Sharing

- DoDI 8320.02 Sharing Data, Info, and IT Services in the DoD
- DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Info Systems
- DoD Information Sharing Strategy
- United States Intelligence Community Information Sharing Strategy
- CJCSI 6211.02D Defense Information System Network: (DISN) Responsibilities
- *CJCSM 3213.02D, Joint Staff Focal Point*

ANTICIPATE

Understand the Battlespace

- FIPS 199 Standards for Security Categorization of Federal Info. and Info. Systems
- NIST SP 800-59 Guideline for Identifying an Information System as a NSS
- NIST SP 800-60, Vol 1, R1 Guide for Mapping Types of Info and Info Systems to Security Categories
- NIST SP 800-92 Guide to Computer Security Log Management
- NIST SP 800-101, R1 Guidelines on Mobile Device Forensics
- NISTIR 7693 Specification for Asset Identification 1.1
- CNSSP-28 Cybersecurity of Unmanned National Security Systems
- DoDI S-5240.23 Counterintelligence (CI) Activities in Cyberspace

Prevent and Delay Attackers and Prevent Attackers from Staying

- FIPS 200 Minimum Security Requirements for Federal Information Systems
- NIST SP 800-37 R1 Guide for Applying the Risk Mgt Framework to Fed. Info. Systems
- NIST SP 800-53 R4 Security & Privacy Controls for Federal Information Systems
- NIST SP 800-53A R4 Assessing Security & Privacy Controls in Fed. Info. Systems & Orgs.
- NIST SP 800-61, R2 Computer Security Incident Handling Guide
- NIST SP 800-124, R1 Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-128 Guide for Security-Focused Configuration Mgt of Info Systems
- CNSSAM IA 1-10, Reducing Risk of Removable Media in NSS
- DoDI 8551.01 Ports, Protocols, and Services Management (PPSM)
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations
- DoD O-8530.1-M CND Service Provider Certification and Accreditation Program
- DoDM 5105.21V1, SCI Admin Security Manual: Info and Info Sys Security
- CJCSI 6510.01F Information Assurance (IA) and Computer Network Defense (CND)
- CJCSM 6510.01B Cyber Incident Handling Program
- *CJCSM 6510.02 IA Vulnerability Mgt Program*
- DTM 17-007, Defense Support to Cyber Incident Response

ABOUT THIS CHART

- This chart organizes cybersecurity policies and guidance by Strategic Goal and Office of Primary Responsibility (see Color Key). Double-clicking on the box directs users to the most authoritative publicly accessible source.
- *Policies in italics indicate the document is marked for limited distribution or no authoritative public-facing hyperlink is currently available.*
- The linked sites are not controlled by the developers of this chart. We check the integrity of the links on a regular basis, but you may occasionally experience an error message due to problems at the source site or the site's decision to move the document. Please let us know if you believe the link is no longer valid.
- CNSS policies link only to the CNSS site, per restrictions implemented by its website design.
- Boxes with red borders reflect recent updates.
- Note: Users of the iPad, iPhone or iPod Touch may find they can view this Chart but that its hyperlinks are inoperable, because of Apple's decision not to fully support certain Adobe products. For those who desire a workaround for this issue, there are apps in the iTunes store for less than $1.00.
- For the latest version of this chart go to http://iac.dtic.mil/csiac/ia_policychart.html. You can sign up to be alerted by e-mail to any updates to this document.

PREPARE

Develop and Maintain Trust

- CNSSP-12 National IA Policy for Space Systems Used to Support NSS
- CNSSP-21 National IA Policy on Enterprise Architectures for NSS
- NSTISSD-600 Communications Security (COMSEC) Monitoring
- CNSSI-5002, National Information Assurance (IA) Instruction for Computerized Telephone Systems
- DoDD 3020.40 Mission Assurance
- DoDD 3100.10 Space Policy
- DoDI 8581.01 IA Policy for Space Systems Used by the DoD
- DoDD 5144.02 DoD Chief Information Officer

Strengthen Cyber Readiness

- NIST SP 800-18, R1 Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-30, R1 Guide for Conducting Risk Assessments
- NIST SP 800-126, R3 SCAP Ver. 1.3
- NIST SP 800-137 Continuous Monitoring
- NIST SP 800-39 Managing Information Security Risk
- DoDD 3700.01 DoD Command and Control (C2) Enabling Capabilities
- DoDD S-3710.01 National Leadership Command Capability
- DoDI 8560.01 COMSEC Monitoring

Sustain Missions

- CNSSP-18 National Policy on Classified Information Spillage
- CNSSP-22, IA Risk Management Policy for National Security Systems
- *CNSSP-300 National Policy on Control of Compromising Emanations*
- CNSSI-1001 National Instruction on Classified Information Spillage
- *CNSSI-4004.1, Destruction and Emergency Protection Procedures for COMSEC and Class. Material*
- *CNSSI-7000 TEMPEST Countermeasures for Facilities*
- *NSTISSI-7001 NONSTOP Countermeasures*
- DoDD 3020.26 DoD Continuity Policy
- DoDD 3020.44 Defense Crisis Management
- DoDI 8410.02 NetOps for the Global Information Grid (GIG)
- Defense Acquisition Guidebook RMF for DoD IT
- *NSA IA Directorate (IAD) Management Directive MD-110 Cryptographic Key Protection*

Color Key - OPRs

🟧	ASD(NII)/ASD(C3I) /DOD CIO	🟦	NIST	⬜	USD(I)
🟫	CNSS/NSTISS	🟩	NSA	🟨	USD(P)
🟦	DISA	🟪	OSD	⬜	USD(P&R)
🟫	DNI	🟪	STRATCOM	⬜	Other Agencies
🟩	JCS	🟥	USD(AT&L)	🟥	Recently updated policy and/or link
🟪	NIAP	🟩	USD(C)	🟨	Expired. Update pending

AUTHORITIES

- Title 10 Armed Forces (§§2224, 3013(b), 5013(b), 8013(b))
- Title 14 Cooperation With Other Agencies (Ch. 7:§§ 141,144,145,148,149,150)
- Title 32 National Guard (§102)
- Title 40 Public Buildings, Property, and Works (Ch. 113: §§11302, 11315, 11331)
- Title 44 Federal Information Security Mod. Act, (Chapter 35)
- Title 50 War and National Defense (§§3002, 1801)
- Clinger-Cohen Act, Pub. L. 104-106
- UCP Unified Command Plan (US Constitution Art II, Title 10 & 50)

NATIONAL / FEDERAL

- Computer Fraud and Abuse Act Title 18 (§1030)
- Federal Wiretap Act Title 18 (§2510 et seq.)
- Stored Communications Act Title 18 (§2701 et seq.)
- Pen Registers and Trap and Trace Devices Title 18 (§3121 et seq.)
- Foreign Intelligence Surveillance Act Title 50 (§1801 et seq)
- Executive Order 13231 as Amended by EO 13286 - Critical Infrastructure Protection in the Info Age
- Executive Order 13526 Classified National Security Information
- Executive Order 13587 Structural Reforms To Improve Classified Nets
- Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing
- NSD 42, National Policy for the Security of Nat'l Security Telecom and Information Systems
- PPD 28, Signals Intelligence Activities
- *NSPD 54 / HSPD 23 Computer Security and Monitoring*
- A-130, Management of Fed Info Resources
- FAR Federal Acquisition Regulation
- Ethics Regulations
- National Strategy to Secure Cyberspace
- NIST Special Publication 800 Series
- NIST SP 800-125A, R1, Security Recommendations for Hypervisor Platforms
- NISTIR 7298, R2, Glossary of Key Information Security Terms
- CNSSD-502 National Directive On Security of National Security Systems
- CNSSD-900, Governing Procedures of the Committee on National Security Systems
- CNSSD-901 Nat'l Security Telecomm's and Info Sys Security (CNSS) Issuance System
- CNSSI-4009 Cmte on National Security Systems Glossary

OPERATIONAL

- *SI 527-01 DoD INFOCON System Procedures*
- *SI 504-04 Readiness Reporting*
- *SI 507-01 NetOps Community of Interest (NCOI) Charter*
- *SI 701-01 NetOps Reporting*
- *STRATCOM CONPLAN 8039-08*
- *STRATCOM OPLANs*
- *Computer Network Directives (CTO, FRAGO, WARNORD)*

SUBORDINATE POLICY

- *Security Configuration Guides (SCGs)*
- *Component-level Policy (Directives, Instructions, Publications, Memoranda)*
- *Security Readiness Review Scripts (SRRs)*
- Security Technical Implementation Guides (STIGs)

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Figure 2.1: Cybersecurity-Policy Domain Including Issuances

Source: https://www.csiac.org/wp-content/uploads/2018/10/cs_policychart.pdf

2.2. Project Focus on Cybersecurity Policy Statement

The Proof-of-Concept case, cybersecurity policy for the smart grid for electric power systems, is important in its own right. It is also a generic component of critical infrastructures, as defined in the 2013 Presidential Policy Directive/PPD-21 on critical infrastructure security and resilience. **[1]**

In the vast policy ecosystem, this Project is best situated in the context of notable policy directives, specifically:

1. *The 2017 Presidential Executive Orders on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" (EO 13800)*,
2. *The 2018 US Department of Defense Cyber Strategy*,
3. *The 2019 National Defense Authorization Act*,
4. *2019 National Intelligence Strategy*.

For illustrative purposes, a brief review, presented in chronological order below, signals features directly relevant to this Project.

2.2.1. *Presidential Executive Order 2017*

In section 2(e) of 2017 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (EO 13800) has ordered the "*assessment of assessment of electricity disruption incident response capabilities*" and "*the readiness of the United States to manage the consequences of such an incident*." **[2]**

In addition, section 1(c) (ii) mandates the use of NIST Cybersecurity Framework to manage cybersecurity risk.

2.2.2. *US DoD Cyber Strategy 2018*

The 2018 DoD Cyber Strategy is based on four pillars. Pillar 1 states: "Build a more lethal joint force strategies" seeks to "leverage automation and data analysis to improve effectiveness", specifically:

> "…The Department will **use cyber enterprise solutions** to operate at machine speed and **large-scale data analytics to identify malicious cyber activity across different networks and systems**. The Department will leverage these advances to improve our own defensive posture and to ensure that our cyber capabilities will continue to be effective against competitors armed with cutting edge technology. **[3]** [Bold added]

The Project contributes to Pillar 2: *"Compete and Deter in Cyberspace"* calls for "*increase the resilience of U.S. critical infrastructure"*:

> "…The Department will work with its interagency and private sector partners to **reduce the risk that malicious cyber activity targeting U.S. critical infrastructure could have catastrophic or cascading consequences**. We will streamline our public-private information-sharing mechanisms and strengthen the resilience and cybersecurity of critical infrastructure networks and systems." **[4]** [Bold added]

Then, too, Pillar 4: “Reform of the Department” seeks to “incorporate cyber awareness into DoD institutional culture”:

> “…The Department will adapt its institutional culture so **individuals at every level are knowledgeable** about the cyberspace domain and can incorporate that knowledge into their day-to-day activities. **Leaders and their staffs need to be “cyber fluent” so they can fully understand the cybersecurity implications of their decisions** and are positioned to identify opportunities to leverage the cyberspace domain to gain strategic, operational, and tactical advantages.” **[4]** [Bold added]

2.2.3. *National Defense Authorization Act 2019*

This Project contributes to the *2019 National Intelligence Strategy of United States of America* **[5]**, specifically the topical mission objective 4 on Cyber Threat Intelligence:

> “Detect and understand cyber threats from state and non-state actors engaged in malicious cyber activity to inform and enable national security decision making, cybersecurity, and the full range of response activities.” **[6]**

Our work is relevant to section 1649 of 2019 National Defense Authorization Act for “pilot program on modeling and simulation in support of military homeland defense operations in connection with cyber-attacks on critical infrastructure.” And further:

> Further to “…carry out a pilot program to **model cyber-attacks on critical infrastructure** in order **to identify and develop means of improving** Department of Defense **responses to requests for defense support** to civil authorities **for such attacks**.” **[7]** [Bold added]

The goal of the Project *maps* onto the requirements as laid out in §1649 of 2019 NDAA, including to “*assess* defense critical infrastructure vulnerabilities and interdependencies to improve military resiliency” and “*determine* the effectiveness of attacks described in subsection (a)(1), and countermeasures, tactics, and tools supporting responsive military homeland defense operations” and others.

2.2.4. *National Intelligence Strategy 2019*

The Project is directly relevant to the *2019 National Intelligence Strategy of United States of America* **[5]**, specifically the topical mission objective 4 on Cyber Threat Intelligence:

> “Detect and understand cyber threats from state and non-state actors engaged in malicious cyber activity to inform and enable national security decision making, cybersecurity, and the full range of response activities.”

Against this background, **Section III** introduces the *Proof-of-Concept* case and the data base. Focused on cybersecurity policy of electrical power smart grids, the purpose is to provide an opportunity for under-the-hood understanding of policies and directives as well as greater appreciation of system component and relationships.

II. COMPLEXITY OF CYBERSECURITY POLICY: References

1. The White House, Office of the Press Secretary. "Presidential Policy Directive – Critical Infrastructure Security and Resilience". Presidential Policy directive/PPD-21. February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

2. United States, Executive Office of the President [Donald Trump]. "Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Federal Register*, 82 FR 22391, pp. 22391-22397. May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

3. Department of Defense, Summary; Donald J. Trump, National Cyber Strategy of the United States of America (Washington, DC: White House, September 2018), p.4. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

4. Department of Defense, Summary; Donald J. Trump, National Cyber Strategy of the United States of America (Washington, DC: White House, September 2018), p.5. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

5. Office of the Director of National Intelligence (2019) *National Intelligence Strategy of the United States of America*, January 23, 2019. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

6. H.R.5515 - 115th Congress (2017-2018) "John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018. p.542. https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

7. H.R.5515 - 115th Congress (2017-2018) "John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018. p.502. https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

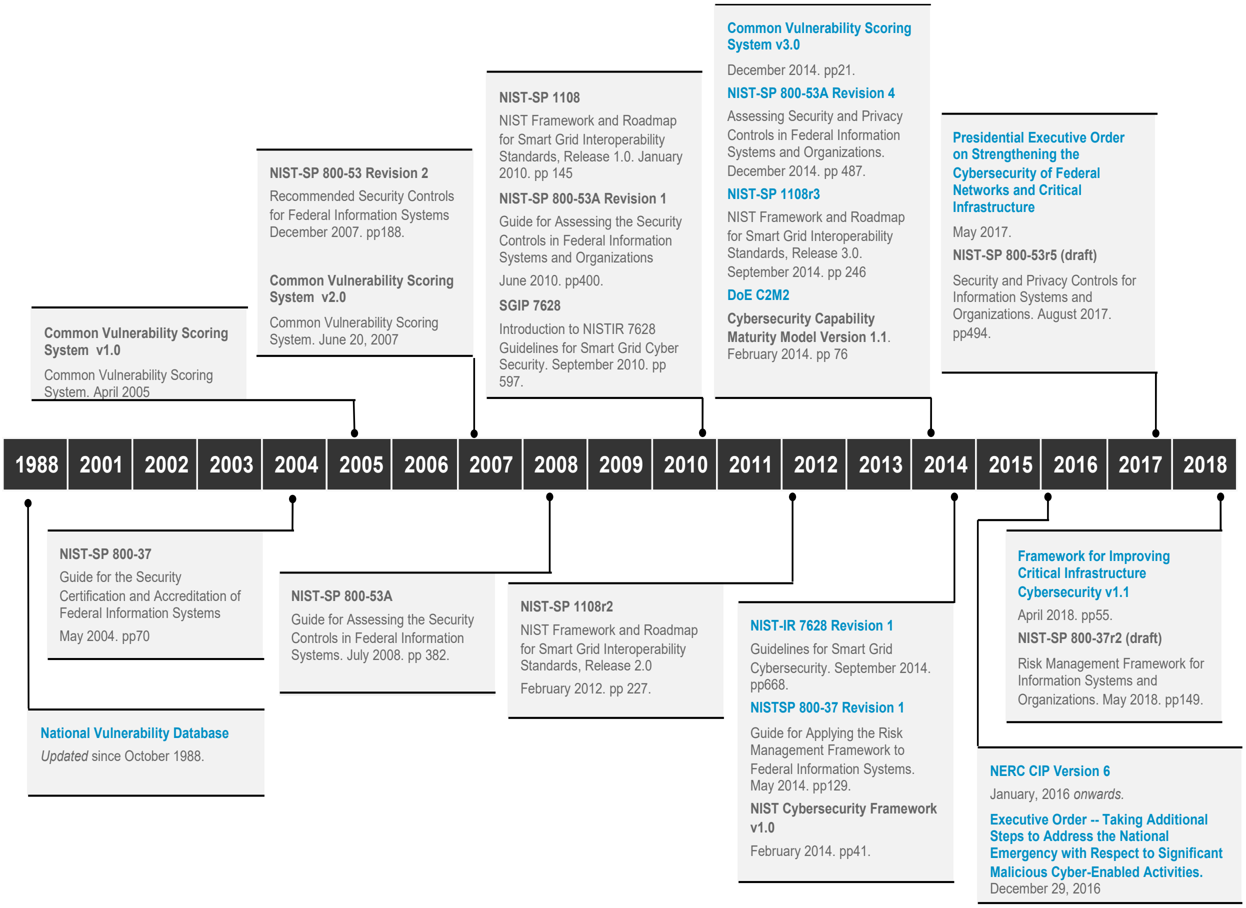
III. POLICY ECOSYSTEM

This Project on the Hard Problem of Policy Governed Secure Collaboration managing cybersecurity risk by capturing the *full-value* of sector or critical infrastructure specific cybersecurity guidelines. The research is framed as a (a) multi-method modular approach, (b) applied to a generic infrastructure system, (c) in a controlled environment.

3.1. The Proof-of-Concept Policy Ecosystem

The "raw data" consists of *National Institute for Standard and Technology* (NIST) guidelines, policies and directives for cybersecurity, augmented by exploration for user-specific customizations and generalizations.

By way of context, **Figure 3.1** shows the development of NIST over a twenty-year period. This development is also an evolution of the focus for institution itself.



Common Vulnerability Scoring System v1.0
Common Vulnerability Scoring System. April 2005
NIST-SP 800-53 Revision 2
Recommended Security Controls for Federal Information Systems December 2007. pp188.
Common Vulnerability Scoring System v2.0
Common Vulnerability Scoring System. June 20, 2007
NIST-SP 1108
NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. January 2010. pp 145
NIST-SP 800-53A Revision 1
Guide for Assessing the Security Controls in Federal Information Systems and Organizations
June 2010. pp400.
SGIP 7628
Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. September 2010. pp 597.
Common Vulnerability Scoring System v3.0
December 2014. pp21.
NIST-SP 800-53A Revision 4
Assessing Security and Privacy Controls in Federal Information Systems and Organizations. December 2014. pp 487.
NIST-SP 1108r3
NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. September 2014. pp 246
DoE C2M2
Cybersecurity Capability Maturity Model Version 1.1. February 2014. pp 76
Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
May 2017.
NIST-SP 800-53r5 (draft)
Security and Privacy Controls for Information Systems and Organizations. August 2017. pp494.
1988
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
NIST-SP 800-37
Guide for the Security Certification and Accreditation of Federal Information Systems
May 2004. pp70
National Vulnerability Database
Updated since October 1988.
NIST-SP 800-53A
Guide for Assessing the Security Controls in Federal Information Systems. July 2008. pp 382.
NIST-SP 1108r2
NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0
February 2012. pp 227.
NIST-IR 7628 Revision 1
Guidelines for Smart Grid Cybersecurity. September 2014. pp668.
NISTSP 800-37 Revision 1
Guide for Applying the Risk Management Framework to Federal Information Systems. May 2014. pp129.
NIST Cybersecurity Framework v1.0
February 2014. pp41.
Framework for Improving Critical Infrastructure Cybersecurity v1.1
April 2018. pp55.
NIST-SP 800-37r2 (draft)
Risk Management Framework for Information Systems and Organizations. May 2018. pp149.
NERC CIP Version 6
January, 2016 onwards.
Executive Order -- Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.
December 29, 2016

Figure 3.1: Evolution of NIST over 1988 – 2018.

In this context, **Figure 3.2** presents a view central to NIST cybersecurity policy ecosystem.

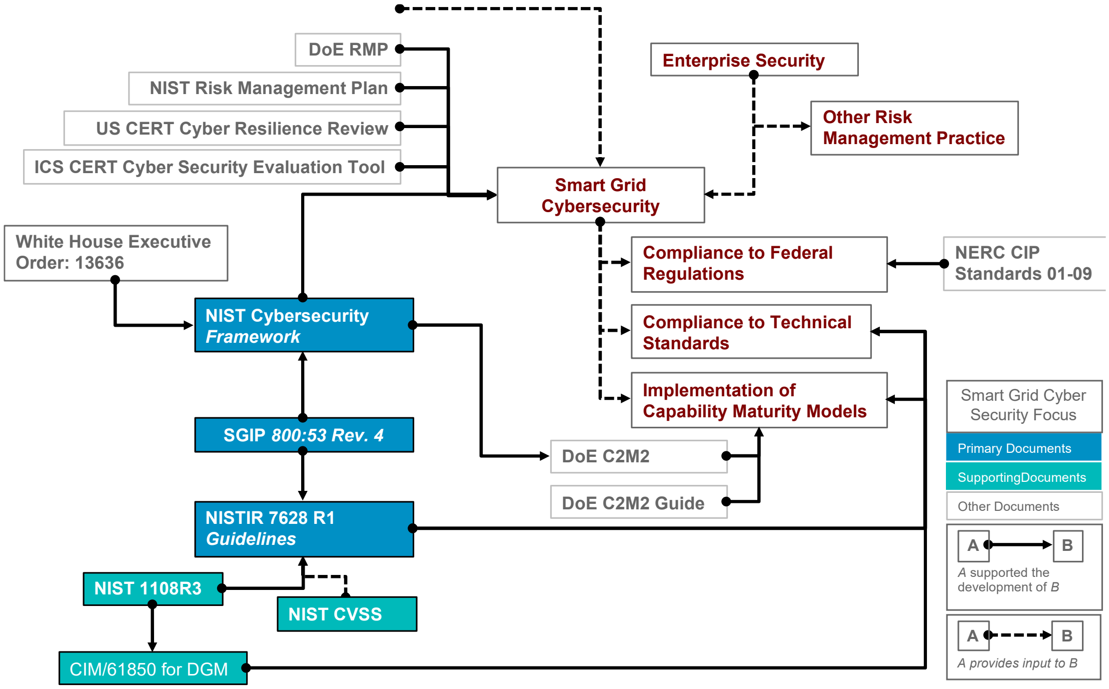

DoE RMP
NIST Risk Management Plan
US CERT Cyber Resilience Review
ICS CERT Cyber Security Evaluation Tool
Enterprise Security
Other Risk Management Practice
Smart Grid Cybersecurity
White House Executive Order: 13636
Compliance to Federal Regulations
NERC CIP Standards 01-09
NIST Cybersecurity Framework
Compliance to Technical Standards
Implementation of Capability Maturity Models
Smart Grid Cyber Security Focus
Primary Documents
SupportingDocuments
Other Documents
SGIP 800:53 Rev. 4
DoE C2M2
DoE C2M2 Guide
NISTIR 7628 R1 Guidelines
A
B
A supported the development of B
NIST 1108R3
NIST CVSS
A
B
A provides input to B
CIM/61850 for DGM

Figure 3.2: NIST Cybersecurity Ecosystem

We selected the cumulative materials in the *NISTIR-7628* on *Guidelines for Smart Grid Cybersecurity* **[1]** as well as the NIST *Cybersecurity Framework (CSF)* **[2]**— all totaling more than 600 pages. Especially important is that these two data-texts are connected via a third policy text namely, NIST *SP 800:53 Rev.4* **[3]** on *Security and Privacy Controls for Federal Information Systems and Organizations*, shown in **Figure 3.3**.

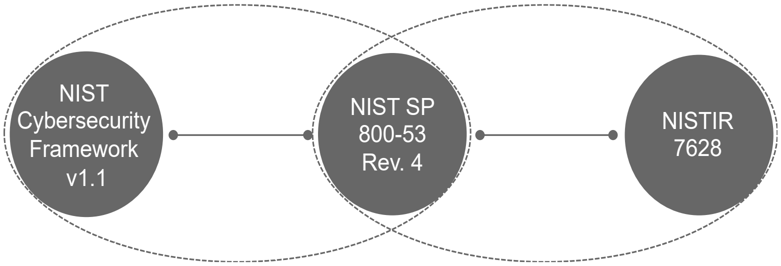


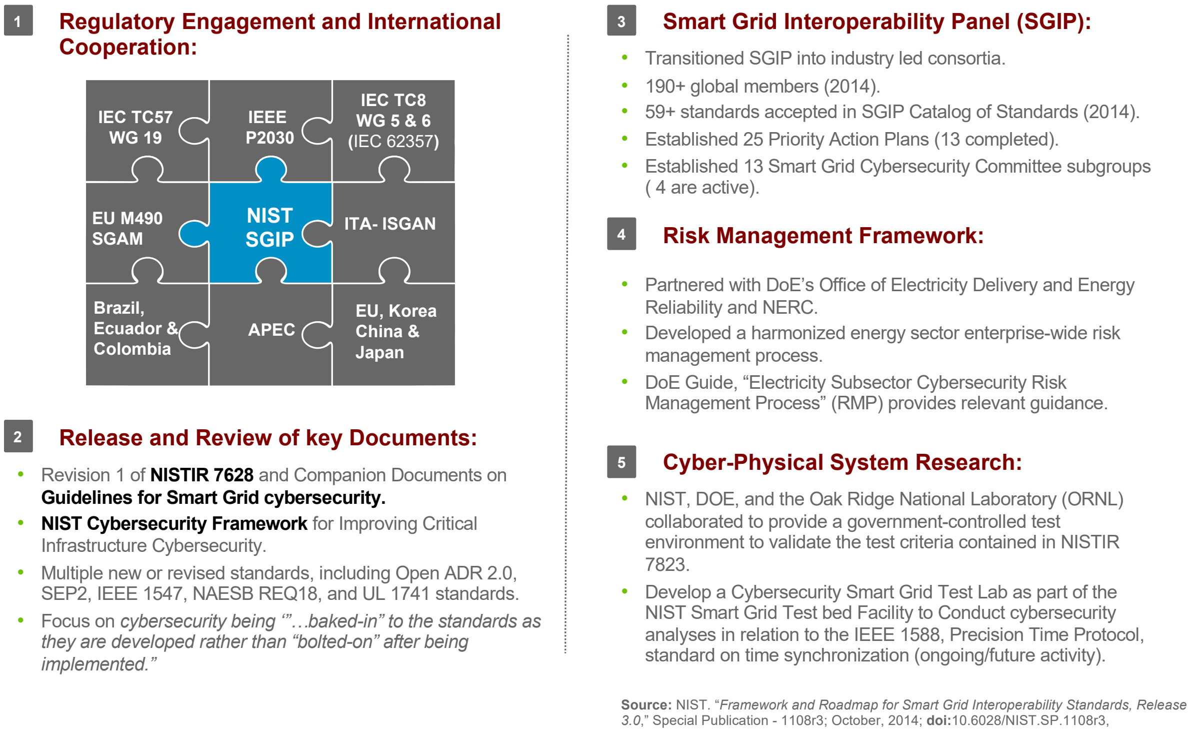
Figure 3.3: Connections of NIST 7628 and NIST CSF

The key point in **Figure 3.3** pertains to the connective function of NIST 800-53 Rev.4 (an issue we shall return to later with Rev.5). We focus on *NISTIR-7628* Guidelines as the text-based raw data, and then augment our investigations with the *NIST Cybersecurity Framework*. The data analysis for this Project has taken placed before the completion of *NIST Cybersecurity Framework* 2.0.

The text-content lineage of *NISTIR 7628* carries fundamental knowledge and provides detailed information on this NIST conceptual representation of smart grid, its actors and activities; the interfaces between actors and their attributes as well as notional views of relationships. These

Figures all help to contextualize the proof-of-concept, the application case, in a broader policy context.

Turning to **Figure 3.4**, we highlight the role of NIST in the specific domain of the *Proof-of-Concept*, namely cybersecurity of smart grid for electrical power systems. The Figure differentiates between documents focused on NIST-cybersecurity for smart grid and those addressing challenges to cybersecurity of critical infrastructure more broadly defined.



1 **Regulatory Engagement and International Cooperation:**

2 **Release and Review of key Documents:**

- Revision 1 of **NISTIR 7628** and Companion Documents on **Guidelines for Smart Grid cybersecurity.**
- **NIST Cybersecurity Framework** for Improving Critical Infrastructure Cybersecurity.
- Multiple new or revised standards, including Open ADR 2.0, SEP2, IEEE 1547, NAESB REQ18, and UL 1741 standards.
- Focus on *cybersecurity being "…baked-in" to the standards as they are developed rather than "bolted-on" after being implemented."*

3 **Smart Grid Interoperability Panel (SGIP):**

- Transitioned SGIP into industry led consortia.
- 190+ global members (2014).
- 59+ standards accepted in SGIP Catalog of Standards (2014).
- Established 25 Priority Action Plans (13 completed).
- Established 13 Smart Grid Cybersecurity Committee subgroups (4 are active).

4 **Risk Management Framework:**

- Partnered with DoE's Office of Electricity Delivery and Energy Reliability and NERC.
- Developed a harmonized energy sector enterprise-wide risk management process.
- DoE Guide, "Electricity Subsector Cybersecurity Risk Management Process" (RMP) provides relevant guidance.

5 **Cyber-Physical System Research:**

- NIST, DOE, and the Oak Ridge National Laboratory (ORNL) collaborated to provide a government-controlled test environment to validate the test criteria contained in NISTIR 7823.
- Develop a Cybersecurity Smart Grid Test Lab as part of the NIST Smart Grid Test bed Facility to Conduct cybersecurity analyses in relation to the IEEE 1588, Precision Time Protocol, standard on time synchronization (ongoing/future activity).

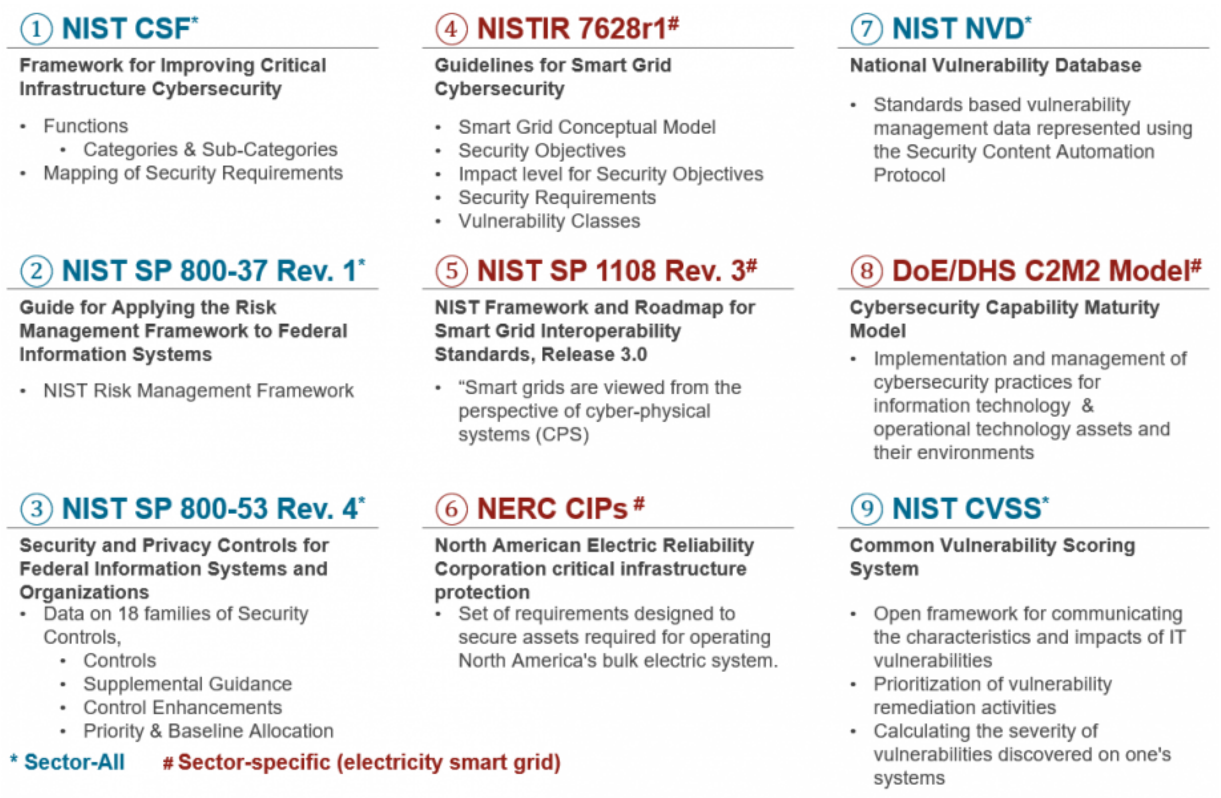
Source: NIST. "*Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*," Special Publication - 1108r3; October, 2014; **doi:**10.6028/NIST.SP.1108r3,

Figure 3.4: Mapping Institutional Context

3.2. Project Data Base

The specific policy documents that serve as core data for the *Proof-of-Concept* are shown in **Figure 3.5.** These texts are of three types:

- *General policy directives* and guideline documents relevant to any system or enterprise (in column 1),
- *Guidelines and directives specific to operations and cybersecurity of smart grid* for electric power systems (column 2), and
- Policy documents for *enterprise specific application* of *NIST Cybersecurity Framework* (as identified in column 1) for the electric smart grid enterprise (as identified in column 3).



① NIST CSF*

Framework for Improving Critical Infrastructure Cybersecurity

- Functions
  - Categories & Sub-Categories
- Mapping of Security Requirements

② NIST SP 800-37 Rev. 1*

Guide for Applying the Risk Management Framework to Federal Information Systems

- NIST Risk Management Framework

③ NIST SP 800-53 Rev. 4*

Security and Privacy Controls for Federal Information Systems and Organizations

- Data on 18 families of Security Controls,
  - Controls
  - Supplemental Guidance
  - Control Enhancements
  - Priority & Baseline Allocation

④ NISTIR 7628r1#

Guidelines for Smart Grid Cybersecurity

- Smart Grid Conceptual Model
- Security Objectives
- Impact level for Security Objectives
- Security Requirements
- Vulnerability Classes

⑤ NIST SP 1108 Rev. 3#

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

- "Smart grids are viewed from the perspective of cyber-physical systems (CPS)

⑥ NERC CIPs #

North American Electric Reliability Corporation critical infrastructure protection

- Set of requirements designed to secure assets required for operating North America's bulk electric system.

⑦ NIST NVD*

National Vulnerability Database

- Standards based vulnerability management data represented using the Security Content Automation Protocol

⑧ DoE/DHS C2M2 Model#

Cybersecurity Capability Maturity Model

- Implementation and management of cybersecurity practices for information technology & operational technology assets and their environments

⑨ NIST CVSS*

Common Vulnerability Scoring System

- Open framework for communicating the characteristics and impacts of IT vulnerabilities
- Prioritization of vulnerability remediation activities
- Calculating the severity of vulnerabilities discovered on one's systems

* Sector-All # Sector-specific (electricity smart grid)

Figure 3.5: Core policy documents for "Text-to-Data"

Note: NIST SP 800-53 Rev.5 is introduced later.

Of the nine policy-responses in **Figure 3.5**, *three* texts noted below explicitly noted in the 2018 DoD Cybersecurity policy and issuances to build and operate a trusted *Department of Defense Information Network* (DoDIN):

1. NIST Cybersecurity Framework

2. NIST SP 800-53 Rev.4: Security and Privacy Controls for Federal Information Systems and Organizations

3. NIST SP 800-37 Rev.1: Guide for Applying the Risk Management Framework to Federal Information Systems

Of the remaining six resources, *three* focus on smart grid, and the other *three* span vulnerability databases, risk quantification methodology and enterprise measurement models. Jointly, these are all the directives whose texts constitute our baseline for metricization.

It is important to stress that the document labelled 800:53 Rev.4 in **Figure 3.5** provides the data that serves the connectivity functions. That function allows us to connect across documents as relevant. *The NIST revision to 800:53 Rev.4 necessitated our "re-do" activities*.

3.3. Essential Data Linkages

The full value of CSF can be difficult to capture given (a) the set of intervening tasks required and (b) the distributed nature of the database. CSF points to ***what*** has to be done and ***why***, but ***not how***. It is up to the user to work through the process outlined by CSF. Pointers to steer users to other (different) documents are provided to assist in next steps.

Because CSF points to a number of individual documents hosting different directives, the users' task is to identify and make connections among them as needed. Moreover, modifications and updates by NIST on the content of key intervening documents require users, in turn, to identify the updates and determine requirements steps.

Against this background, we introduce **Figure 3.6** that situates NIST directives and guidelines within segments of the broader ecosystem designed to support smart grid cybersecurity. The Figure also serves to locate our Project in a broader cybersecurity policy context.

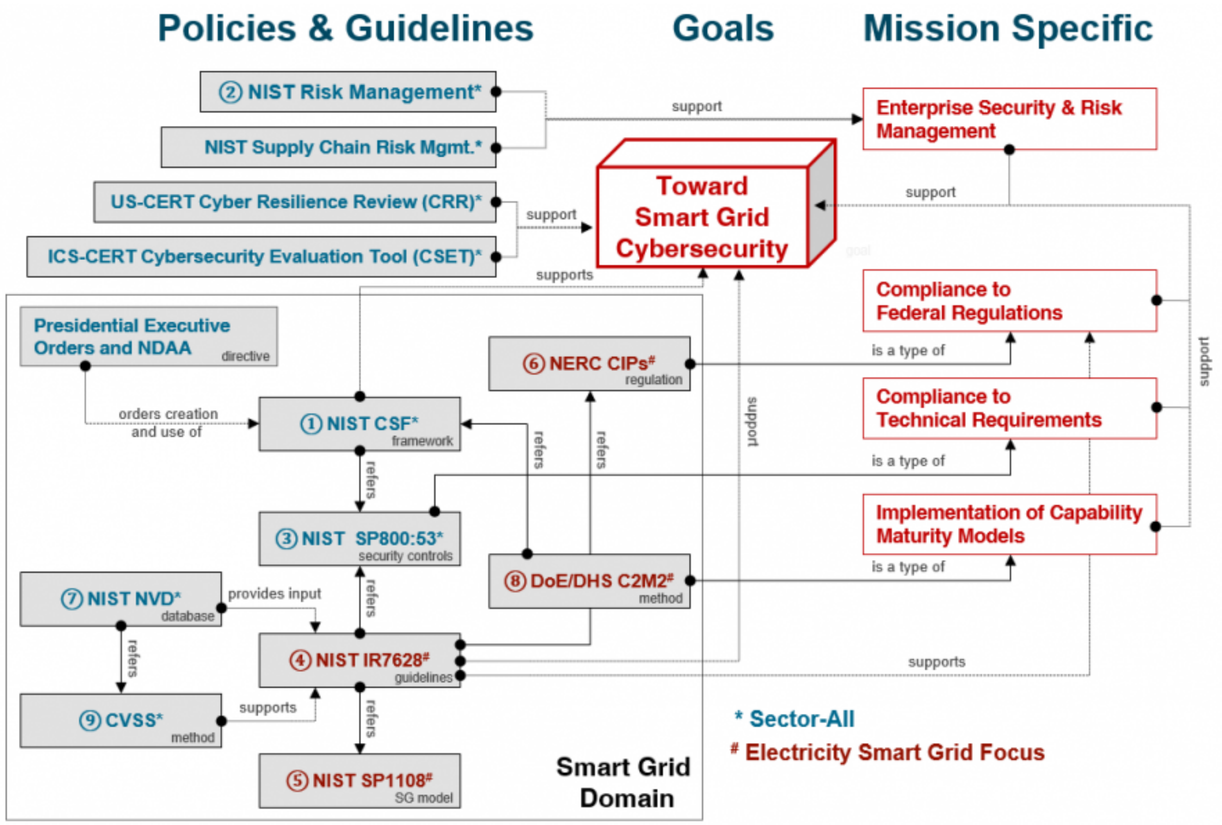


Figure 3.6: Smart Grid CPS cybersecurity policy ecosystem

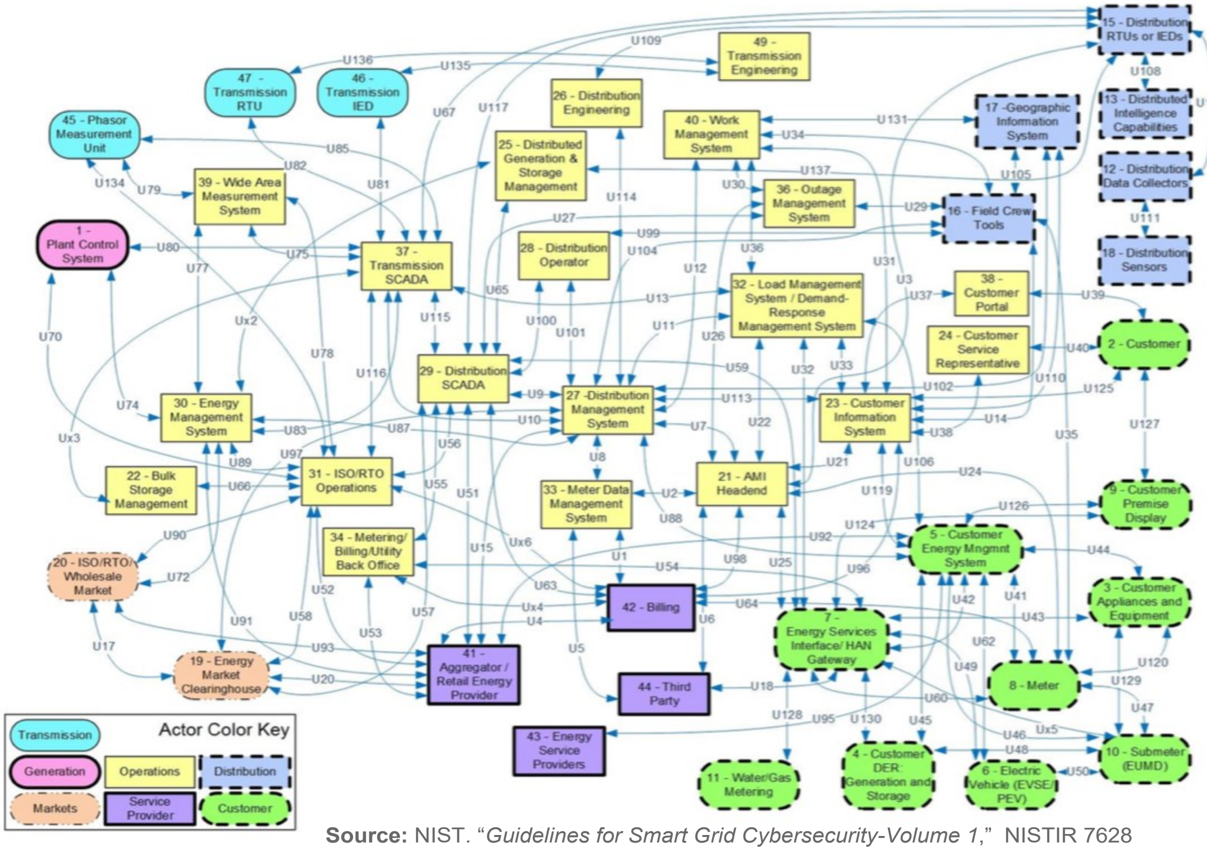
Note: See **Figure 3.5** for identification of documents indicated by circled number. Framed by Gaurav Agarwal [aka Gaurav]

3.4. The Cyber-Physical System: “As is” State

At this point, we turn to the *method* developed in this Project to generate “raw-data”, and to build the data-set required for metricization. The method is presented as sequential Steps – one at a time:

Our purpose is to provide a more user-friendly operational approach to the contents of the conceptual model. We do so by organizing the overall system structure and process in order to yield a coherent framework of the system” as is”, as well as to assist in situating the fundamental vulnerabilities and security objectives.

Step One focuses on the *NIST Conceptual Model for Smart Grid*. **Figure 3.7** – extracted from *NISTIR 7628 Guidelines for Smart Grid Cybersecurity* – shows the NIST’s “Smart Grid conceptual model”, and its constituent elements, defined as (1) *actors and domains* and (2) *logical interfaces*. It is shown here to indicate the richness of the NIST framing.



15 - Distribution RTUs or IEDs
49 - Transmission Engineering
47 - Transmission RTU
46 - Transmission IED
26 - Distribution Engineering
45 - Phasor Measurement Unit
25 - Distributed Generation & Storage Management
40 - Work Management System
17 -Geographic Information System
13 - Distributed Intelligence Capabilities
39 - Wide Area Measurement System
12 - Distribution Data Collectors
36 - Outage Management System
16 - Field Crew Tools
1 - Plant Control System
37 - Transmission SCADA
28 - Distribution Operator
18 - Distribution Sensors
32 - Load Management System / Demand-Response Management System
38 - Customer Portal
24 - Customer Service Representative
2 - Customer
29 - Distribution SCADA
27 -Distribution Management System
30 - Energy Management System
23 - Customer Information System
22 - Bulk Storage Management
31 - ISO/RTO Operations
33 - Meter Data Management System
21 - AMI Headend
9 - Customer Premise Display
34 - Metering/ Billing/Utility Back Office
5 - Customer Energy Mngmnt System
20 - ISO/RTO Wholesale Market
42 - Billing
3 - Customer Appliances and Equipment
7 - Energy Services Interface/ HAN Gateway
19 - Energy Market Clearinghouse
41 - Aggregator / Retail Energy Provider
44 - Third Party
8 - Meter
43 - Energy Service Providers
11 - Water/Gas Metering
4 - Customer DER: Generation and Storage
6 - Electric Vehicle (EVSE/ PEV)
10 - Submeter (EUMD)
Actor Color Key
Transmission
Generation
Operations
Distribution
Markets
Service Provider
Customer

Source: NIST. “*Guidelines for Smart Grid Cybersecurity-Volume 1*,” NISTIR 7628 Revision I, September, 2014.

Figure 3.7: NIST Conceptual Model for Smart Grid

Source: NISTIR 7628 Rev.1 *Guidelines for Smart Grid Cybersecurity*. **[1]**

This NIST “model” provides the anchor or entry point for building our data base of (a) domains and actors, and (b) logical interfaces:

3.4.1. *Domains and Actors*

The NIST Model consists of:

- **7 Domains:** *Domains* encompass smart grid conceptual roles and services. It includes types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing identified goals.

- **47 Actors:** *Actors* may be devices, computer systems or software programs and/or the organizations that own them. Actors have the capability to make decisions and exchange information with other actors through interfaces. Each actor has one or more roles. It is the usual or expected function, capability of, or service played by an actor, or the part played in a particular action or event.

3.4.2. *Logical Interfaces*

The NIST Model consists of:

- **130 Logical** Interface between Actors: *Interfaces* represent the point of access between domains. Interfaces show either electrical connections or communications connections. Each of these interfaces may be bidirectional. Communications interfaces represent an information exchange between two domains and the actors within; they do not represent physical connections. They represent logical connections in the smart grid information network interconnecting various domains.

- **22 Categories** of Logical Interface: As many individual logical interfaces have similar security-related characteristics, they are categorized together as a means to simplify the identification of the appropriate security requirements. These security-related logical interface categories are defined based on attributes that could affect the security requirements.

- **18 attributes** of Logical Interface Category: Key attributes include requirements and constraints that are used in the determination of impact level for three security objectives, and selection of security requirements for the logical interface category.

Step one concludes use of, and reference to, **Figure 3.7** from the infrastructure specific *NISTIR 7628 Guidelines for Smart Grid Cybersecurity* to construct the “As Is” system model.

The following steps build upon this basic foundation. The goal is to identify the vulnerability and related conditions, and then connect these to the “As Is” system model.

3.5. Vulnerabilities of the “As Is” System

Step Two is based on materials provided by *NISTIR 7628* on system vulnerabilities presented in the following texts:

- NIST Special Publication (SP) 800-82 Revision 1 Guide to Industrial Control Systems Security **[4]**;

- NIST 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations **[5]**;

- Open Web Application Security Project (OWASP) vulnerabilities **[6]**;
- Common Weakness Enumeration (CWE) vulnerabilities **[7]**;
- Attack documentation from Idaho National Laboratory (INL);
- Input provided by the NIST CSWG Bottom-Up group; and
- the North American Electric Reliability Corporation Critical Infrastructure Protection Standards (NERC CIP) **[8]**.

NISTIR-7628 also reports the construction of a set of vulnerability types from these multiple sources consisting of **53 types of vulnerabilities**, clustered in **4 categories**:

- People, policy and procedure;
- Platform software/firmware vulnerabilities;
- Platform vulnerabilities; and
- Network factors.

3.6. Security Objectives – of "As Is"

Step Three focuses on the security objectives and the impact levels for the smart grid with the well-known C-I-A defined as follows:

- **Availability** of the grid as primary requirement**:** "Ensuring timely and reliable access to and use of information...." [44 U.S.C., Sec. 3542, p.148] **[9].**

- **Integrity** of information as secondary but increasingly critical requirement and the "guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity...." [44 U.S.C., Sec. 3542, p.147] **[10].**

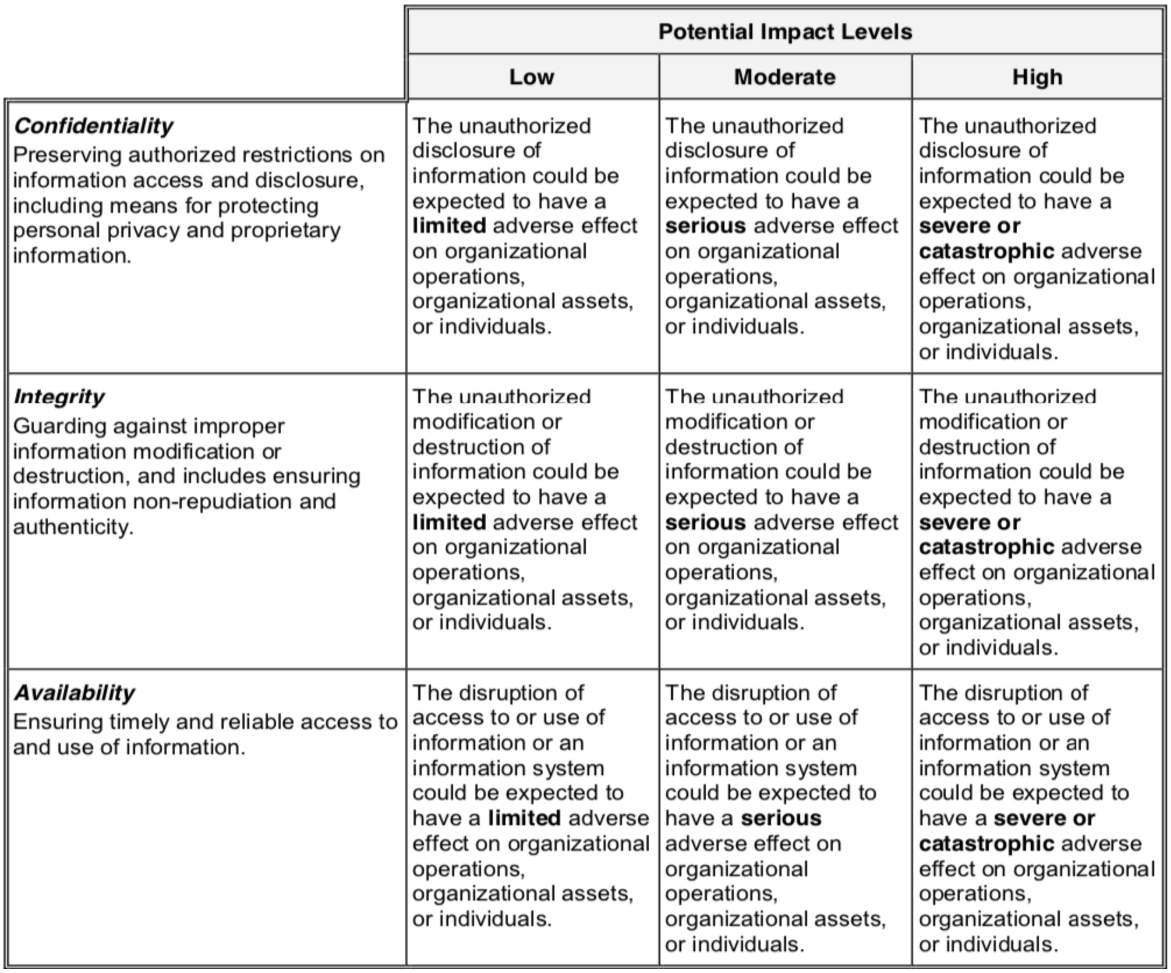
- **Confidentiality** of customer information for revenue billing and privacy concerns. NISTIR 7628 uses the definitions for the security objectives of C.I.A., defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...." [44 U.S.C., Sec. 3542, p. 148] **[9].**

The impact level on the logical interfaces is then recorded for *each* of the security objectives. The individual impact level (i.e., low, moderate, high) is based upon the expected adverse effect of a security breach upon organizational operations, organizational assets, or individuals.

NISTIR 7628 **[1]** employs the definitions in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* **[11]** for impact levels for each security objective.

Table 3.1 presents the definition of the potential Impact levels for each of C-I-A.

Table 3.1: Impact levels definitions



	Potential Impact Levels		
	Low	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Source: NISTIR 7628 Rev.1 Guidelines for Smart Grid Cybersecurity **[1]**

3.7. Security Requirements

Step Four then characterizes the security requirements for the system overall. These are organized in clusters and in categories:

- **19 clusters of over 180 Security** Requirements available from several sources: NIST SP 800-53 **[3]**, the DHS Catalog **[12]**, NERC CIPs **[8]**, and the NRC Regulatory Guidance **[13]** that are organized into families primarily based on NIST SP 800-53 **[3]**.

- **Categories of Security Requirements:** Each security requirement is allocated to one of three categories:

  - *Governance, Risk, and Compliance (GRC)* whereby such requirements are addressed at organizational level. They are centered around policy, procedure, and compliance-based activities.

  - *Common Technical Requirements* applicable to all the logical interface categories.

- *Unique Technical Requirements* allocated to one or more of the logical interface categories.

These security requirements are applicable at any logical interface of the "As Is" system model.

3.8. Cybersecurity Activities – Mapping Task

Step Five centers on Proof-of-Concept case, NIST IR 7628 Rev.1: *Guidelines for Smart Grid Cybersecurity*. In this context. **Figure 3.8** identifies the five main *functions* of the NIST *Cybersecurity Framework* (*Identify*, *Protect*, *Detect*, *Respond* and *Recover*). These functions define the basic cybersecurity activities at their highest level of aggregation. They are designed to assist an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

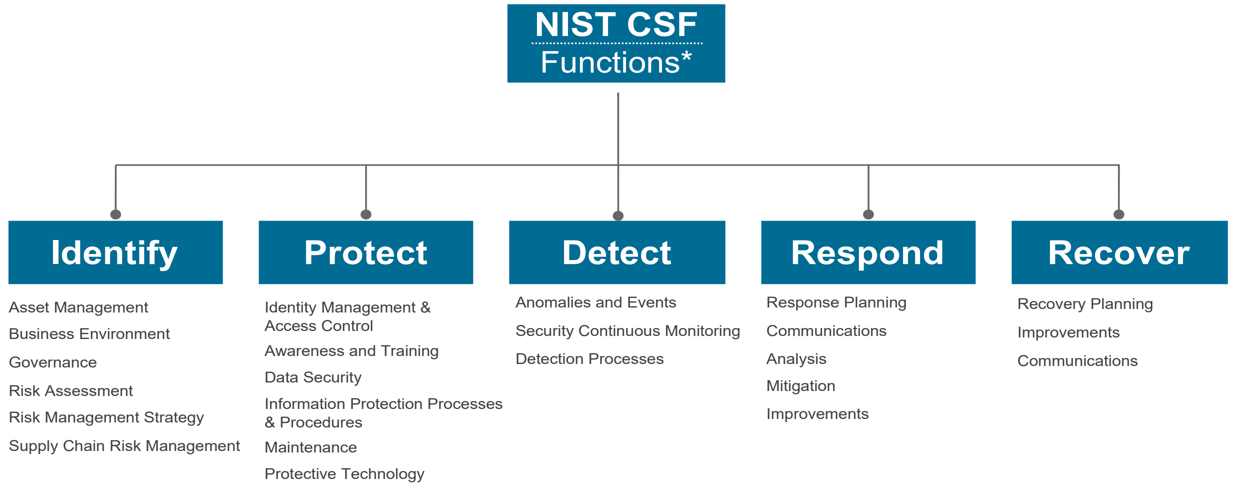


Figure 3.8: Functions and Categories of NIST Cybersecurity Framework

Source: Based on NIST Cybersecurity Framework. **[2]**

The NIST *Cybersecurity Framework* (NIST CSF) **[2]** is *generic* in form, that is, with relevance to all types of critical infrastructures. We augment the database by extracting from CSF those features deemed as generic and directly applicable to the smart grid as our application of a critical infrastructure. Given that the NIST CSF was developed after the release of NISTIR 7628, these two documents are on independent of each other.

3.9. Connective Mapping

Step six consists of connecting the security requirements provided in NIST 7628 **[1]** and NIST CSF **[2]**. The *connective mapping* is based on security requirements provided in NIST SP 800:53 Rev.4 **[3]**.

Then, in order to complete **Step Six** and connect the outcomes associated with each sub-category, NIST CSF makes informative references to sections of standards, guidelines, and practices including NIST SP 800-53 Rev.4. We use NIST SP 800-53 Rev.4 to map the applicability of NIST CSF to logical interfaces and actors of Smart Grid conceptual Model. (Further along, we turn to the use of Rev.5.)

When completed, this *connective mapping* facilitates the understanding and tracking of all system operations, components, vulnerabilities and the like, that bear upon specific elements in the *infrastructure-specific system*. These are augmented with the application of relevant *generic features* of the Cybersecurity Framework.

3.10. Result – Raw Data Base

The product of these ***Six Steps*** is a structured "As Is" system model based on a sequential logic – and starting with core system feature, followed by vulnerabilities, then security objectives etc. The process yields a cumulative "onion like" database. The "raw data", grouped into three segments, is shown in **Table 3.2** below.

Table 3.2: Summary of characteristic features of raw database

The Raw Data Base is:
Anchored in: **"As Is State" of Infrastructure Specific System**
• **Actor and domain (or function)**
• **Logical interfaces**
Augmented by: **Vulnerabilities, Security Objectives, Impacts, Requirements**
• **Vulnerabilities for each of actors and domains**
• **Security objectives**
• **Impact for each of the three-security objectives of system**
Availability, information integrity and customer confidentiality
• **Applicable Security requirements**
Augmented by: **Customized application of Cybersecurity Framework to "As Is State"**
• **Applicable sub-categories, categories and functions of NIST Cybersecurity Framework.**

At this point most of the "pieces" of data-making are in place, and we can now summarize the *rules for data-extraction*.

3.11. Summary of Rules for Text-to-data

The data-extraction and linkage strategy are shown in **Figure 3.9.** This Figure provides a high-level view of the vastness of the information embedded in *NISTIR-7628* (and its supporting texts). It is designed to show the *linkage-strategy* that connect the components of policy-governed security for cyber-physical systems.

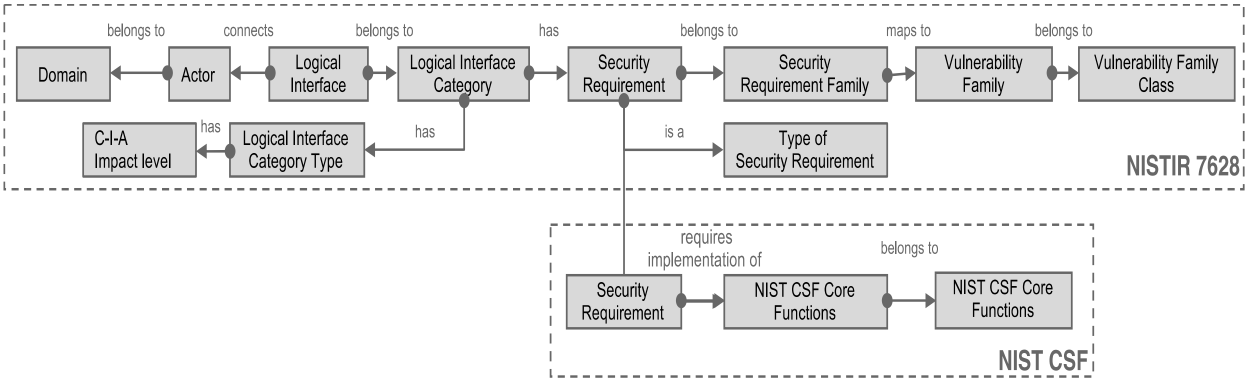


Figure 3.9: The extraction and overall linkage strategy

Framed by Gaurav Agarwal [aka Gaurav]

Section IV focuses on the *Proof-of-Concept* processes – notably from text-to-data, from data-to-framework, from framework-to-metrics, and from metrics-to-model.

III. POLICY ECOSYSTEM: References

1. National Institute of Standards and Technology (2020) *Guidelines for Smart Grid Cybersecurity*. (U.S. Department of Commerce, Washington, D.C.), Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, NISTIR 7628, Vol.1, REV.1. September 2014. https://doi.org/10.6028/NIST.IR.7628r1

2. National Institute of Standards and Technology (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, https://doi.org/10.6028/NIST.CSWP.04162018

3. National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53) (Rev. 4) (April, 2013) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

4. NIST Special Publication (SP) 800-82 Revision 1 Guide to Industrial Control Systems Security. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

5. NIST 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations. (April, 2013) https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf

6. Open Web Application Security Project (OWASP) vulnerabilities. https://www.owasp.org

7. Common Weakness Enumeration (CWE) vulnerabilities. https://cwe.mitre.org

8. North American Electric Reliability Corporation (NERC), United States Mandatory Standards Subject to Enforcement: Critical Infrastructure Protection (CIP) Standards [Web page], http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20State

9. United States Code, 2012 Edition, Supplement 1, Title 44 - PUBLIC PRINTING AND DOCUMENTS. Added Pub. L. 107-347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947. p.148

10. United States Code, 2012 Edition, Supplement 1, Title 44 - PUBLIC PRINTING AND DOCUMENTS. Added Pub. L. 107-347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947. p.147

11. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

12. The National Infrastructure Protection Plan, Partnering to enhance protection and resiliency, Department of Homeland Security (DHS), 2009.

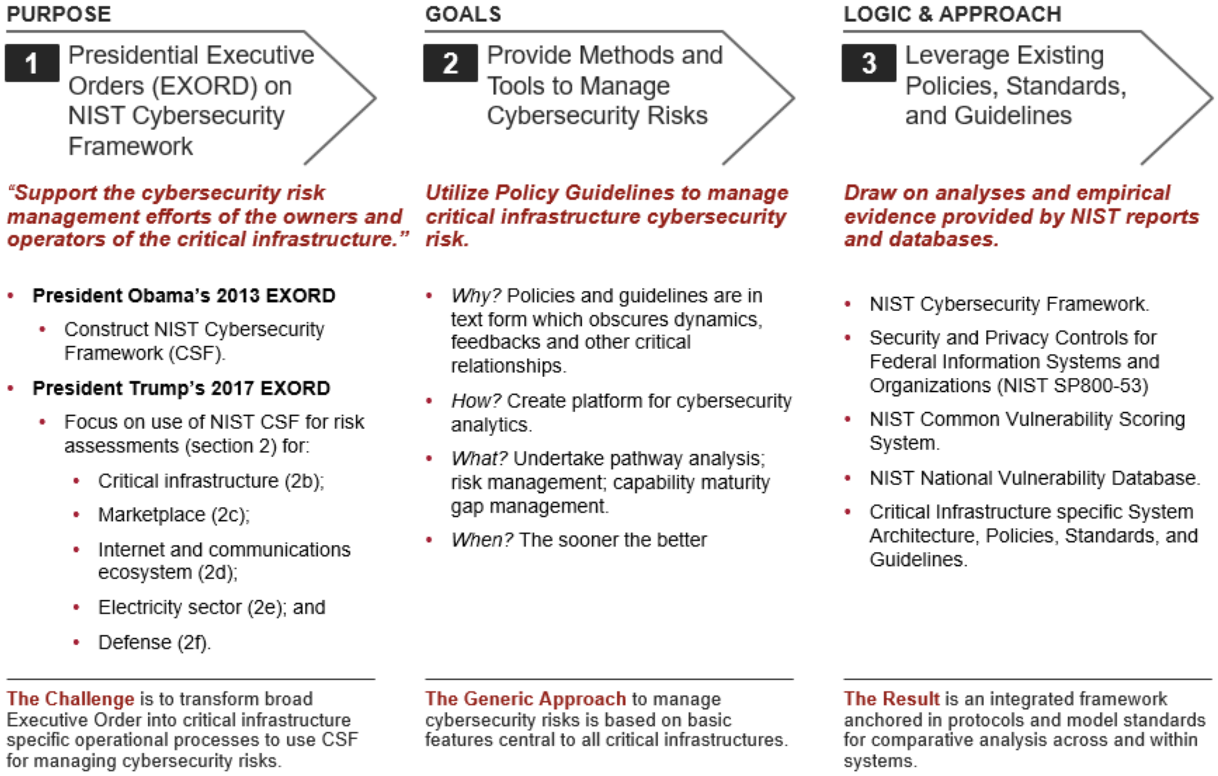
13. NRC Regulatory Guidance: Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment, version 1.0, NERC, June 14, 2002.

IV. PROOF-of-CONCEPT

Early in the research design, we sought to align our Project with national policy by consolidating our vision and mission around EXORD and NDAA statements. This task is designed to ensure that research remains anchored in national policy priorities.

4.1. Alignment with National Cybersecurity Policy

In order to avoid losing sight of the "big picture" when we delve into details later on, **Figures 4.1a** and **4.1b** provide a high-level view of both vision and mission. Embedded in these Figures is also a more detailed accounting of our orientation with respect to purpose and goals, and logic and approach.



PURPOSE

1 Presidential Executive Orders (EXORD) on NIST Cybersecurity Framework

"Support the cybersecurity risk management efforts of the owners and operators of the critical infrastructure."

- **President Obama's 2013 EXORD**
  - Construct NIST Cybersecurity Framework (CSF).
- **President Trump's 2017 EXORD**
  - Focus on use of NIST CSF for risk assessments (section 2) for:
    - Critical infrastructure (2b);
    - Marketplace (2c);
    - Internet and communications ecosystem (2d);
    - Electricity sector (2e); and
    - Defense (2f).

The Challenge is to transform broad Executive Order into critical infrastructure specific operational processes to use CSF for managing cybersecurity risks.

GOALS

2 Provide Methods and Tools to Manage Cybersecurity Risks

Utilize Policy Guidelines to manage critical infrastructure cybersecurity risk.

- *Why?* Policies and guidelines are in text form which obscures dynamics, feedbacks and other critical relationships.
- *How?* Create platform for cybersecurity analytics.
- *What?* Undertake pathway analysis; risk management; capability maturity gap management.
- *When?* The sooner the better

The Generic Approach to manage cybersecurity risks is based on basic features central to all critical infrastructures.

LOGIC & APPROACH

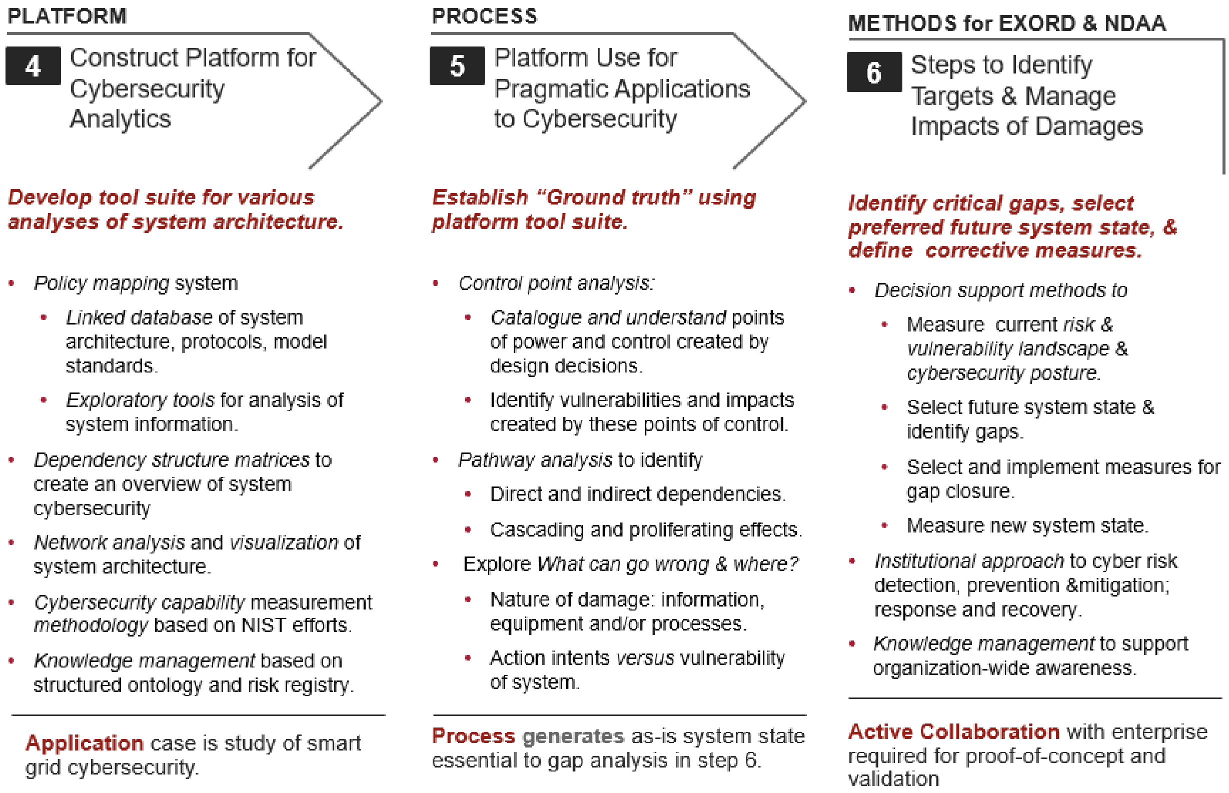
3 Leverage Existing Policies, Standards, and Guidelines

Draw on analyses and empirical evidence provided by NIST reports and databases.

- NIST Cybersecurity Framework.
- Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP800-53)
- NIST Common Vulnerability Scoring System.
- NIST National Vulnerability Database.
- Critical Infrastructure specific System Architecture, Policies, Standards, and Guidelines.

The Result is an integrated framework anchored in protocols and model standards for comparative analysis across and within systems.

Figure 4.1a: Support for national cybersecurity policies - vision and mission



PLATFORM

4 Construct Platform for Cybersecurity Analytics

Develop tool suite for various analyses of system architecture.

- *Policy mapping* system
  - *Linked database* of system architecture, protocols, model standards.
  - *Exploratory tools* for analysis of system information.
- *Dependency structure matrices* to create an overview of system cybersecurity
- *Network analysis* and *visualization* of system architecture.
- *Cybersecurity capability* measurement *methodology* based on NIST efforts.
- *Knowledge management* based on structured ontology and risk registry.

Application case is study of smart grid cybersecurity.

PROCESS

5 Platform Use for Pragmatic Applications to Cybersecurity

Establish "Ground truth" using platform tool suite.

- *Control point analysis:*
  - *Catalogue and understand* points of power and control created by design decisions.
  - Identify vulnerabilities and impacts created by these points of control.
- *Pathway analysis* to identify
  - Direct and indirect dependencies.
  - Cascading and proliferating effects.
- Explore *What can go wrong & where?*
  - Nature of damage: information, equipment and/or processes.
  - Action intents *versus* vulnerability of system.

Process generates as-is system state essential to gap analysis in step 6.

METHODS for EXORD & NDAA

6 Steps to Identify Targets & Manage Impacts of Damages

Identify critical gaps, select preferred future system state, & define corrective measures.

- *Decision support methods to*
  - Measure current *risk & vulnerability landscape* & *cybersecurity posture.*
  - Select future system state & identify gaps.
  - Select and implement measures for gap closure.
  - Measure new system state.
- *Institutional approach* to cyber risk detection, prevention &mitigation; response and recovery.
- *Knowledge management* to support organization-wide awareness.

Active Collaboration with enterprise required for proof-of-concept and validation

Figure 4.1b: Support for national cybersecurity policies - activities and outcomes

The following parts of **Section IV** provide a brief review of process and present some results for the *Proof-of-Concept* case – with its focus on cybersecurity for smart grid of electrical power systems.

4.2. Review of Process

The research design, organized in modular terms, begins with the properties of a structured model for complex cyber-physical systems. The design and analyses are generic in the sense that they are relevant to, and provide insights for, the cybersecurity of various complex cyber-physical systems.

Table 4.1 presents an organized summary for the process of constructing structured data from text. The numbers following each step serve as identifiers of the information sources in **Figure 3.5** earlier.

Table 4.1: Structured Data for CPS Analytics

1	**As-Is System State**	▪ Construct frame for "as-is" Smart Grid Reference Model of *Actors* & *Domains* ⑤. ▪ Identify *Logical information Interfaces* ④ between actors & their *Interface categories* ④ of Smart Grid NIST Model.
2	**System Vulnerabilities**	▪ Include *vulnerabilities* ⑦ of the "as is" Smart Grid system. ▪ Classify vulnerabilities into *types & families* ④. ▪ Construct composite *exploitability metric* ⑨ for each vulnerability.
3	**Security Objective Impact Level**	▪ Determine confidentiality, integrity, & availability *impact level* ④ of logical interfaces. ▪ Construct composite *impact metric* ⑨ for each logical interface.
4	**Security Requirements**	▪ Identify *security requirements* ④ for each logical interface. ▪ Identify *Security and Privacy controls* ③, and *critical Infrastructure plans* ⑥.
5	**Mission-Specific Requirements**	▪ Identify *cybersecurity framework functions and categories* ①. ▪ Align & prioritize cybersecurity activities with mission requirements, risk tolerances, & resources through use of *cyber capability & maturity model* ⑧, & *risk management framework* ②.

The *Cybersecurity Framework* is mandatory in the public sector and greatly encouraged for the private sector. However, the mission-specific application is left to the user—with only general guidance provided by CSF directives. It is up to the user to proceed as best determined.

We situate the results shown below at the *interface of users* and *CSF* in order to facilitate access to, and use of, CSF. The general purpose here is to help users and, in the process, to provide tools to explore mission-related properties, concerns, or contingencies.

For this reason, we have designed the entire project in modular terms, based on a *structured model* of system properties. Different users may prefer to use different features and/or draw on results (or products) generated at different phases of this project.

4.3. Policy Linkage Process – Reminder

The ***Text-to-Data*** task yields a linked database of nine policy documents. The linked database, from the nine documents, consists of a set of variables that represent:

- ***System State***, "As-Is," focusing on system actors and activities (labelled as nodes) and logical interfaces among them,
- ***Vulnerability Classes*** that may affect a node or logical interface,
- ***Security Objectives***, as stated by NIST,
- ***Impact Level*** on nodes and logical interfaces,
- ***Connections*** and logical interface(s) between two nodes,
- ***Security Requirements*** for nodes and logical interfaces, and
- ***Cybersecurity Framework Functions*** applied between each two nodes.

4.4. Data to Framework

The “As Is” system model of the cyber-physical system is generated by the process of ***Data-to-Framework***. The process consists of creating a Design Structure Matrix (DSM) to: (a) construct an internally consistent framework for organizing, metricizing, and managing critical information, and (b) create an initial, baseline, for subsequent models of the cyber-physical system.

The DSM in **Figure 4.2** represents the system “As-Is” for the core of the NIST smart grid defined by *Actors and Domains*. (Actors are located in the rows and columns; and Actors in the same domain are bound by a box.) The DSM is a structured transformation of the NIST Figure in the inset. The inset is a copy of **Figure 3.7** shown earlier, presented again here as a reminder. The DSM, also known as dependency structure matrix, provides the Framework within which the properties of the system are recorded.

4.5. Framework to Metrics

Once we examine system structure and process of information flows, technical architecture, and system management, the research design calls us to:

- Analyze the system-wide structure and information flows,
- Generate visual representations of structure and information flows using graph theory and network methods,
- Use these representations to identify critical nodal or control points (direct or indirect) that may be targets for unwanted interventions, and to the extent possible,
- Distinguish between human/management and technical/operations.

Following the CSF directives (Noted in **Figure 4.1**) we identify empirically key properties of the logical interfaces for the system “As Is” namely:

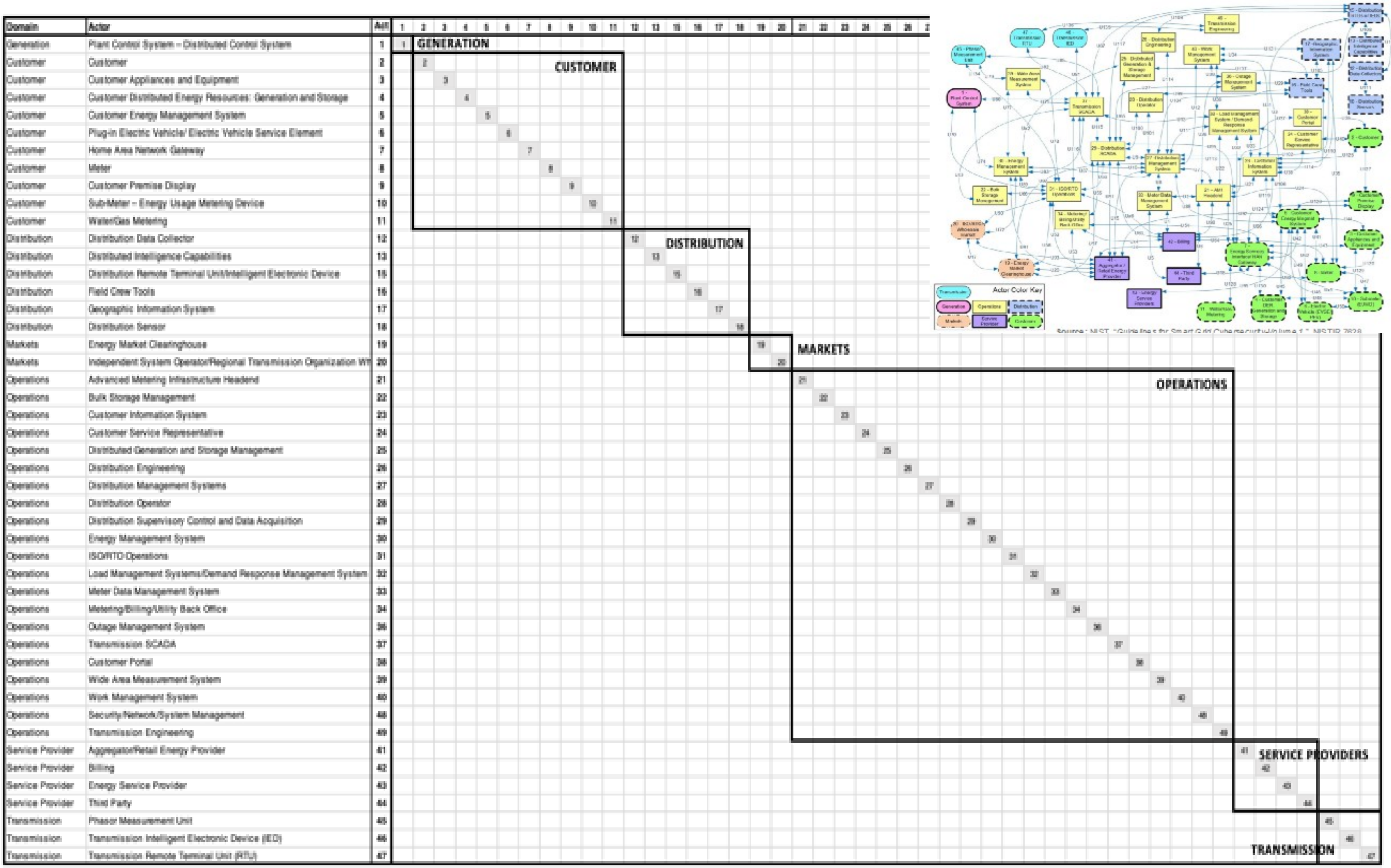
i. ***Impact levels*** for each Confidentiality, Integrity, Availability security objective (C-I-A),

ii. ***Security requirements*** based on Impact level for each C-I-A security objective,

iii. ***Cybersecurity Framework*** *functions* based on Impact level.

This work enhances and enriches our database, and transcends analysis of the “system as is.”

Figure 4.3 follows immediately from the above, and presents the *logical interfaces* among actors embedded in a domain. This Figure provides the inputs for the network model of the *Proof-of-Concept* as the cyber-physical system in point.



Domain	Actor	Act#
Generation	Plant Control System – Distributed Control System	1
Customer	Customer	2
Customer	Customer Appliances and Equipment	3
Customer	Customer Distributed Energy Resources: Generation and Storage	4
Customer	Customer Energy Management System	5
Customer	Plug-in Electric Vehicle/ Electric Vehicle Service Element	6
Customer	Home Area Network Gateway	7
Customer	Meter	8
Customer	Customer Premise Display	9
Customer	Sub-Meter – Energy Usage Metering Device	10
Customer	Water/Gas Metering	11
Distribution	Distribution Data Collector	12
Distribution	Distributed Intelligence Capabilities	13
Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	15
Distribution	Field Crew Tools	16
Distribution	Geographic Information System	17
Distribution	Distribution Sensor	18
Markets	Energy Market Clearinghouse	19
Markets	Independent System Operator/Regional Transmission Organization Wh	20
Operations	Advanced Metering Infrastructure Headend	21
Operations	Bulk Storage Management	22
Operations	Customer Information System	23
Operations	Customer Service Representative	24
Operations	Distributed Generation and Storage Management	25
Operations	Distribution Engineering	26
Operations	Distribution Management Systems	27
Operations	Distribution Operator	28
Operations	Distribution Supervisory Control and Data Acquisition	29
Operations	Energy Management System	30
Operations	ISO/RTO Operations	31
Operations	Load Management Systems/Demand Response Management System	32
Operations	Meter Data Management System	33
Operations	Metering/Billing/Utility Back Office	34
Operations	Outage Management System	36
Operations	Transmission SCADA	37
Operations	Customer Portal	38
Operations	Wide Area Measurement System	39
Operations	Work Management System	40
Operations	Security/Network/System Management	48
Operations	Transmission Engineering	49
Service Provider	Aggregator/Retail Energy Provider	41
Service Provider	Billing	42
Service Provider	Energy Service Provider	43
Service Provider	Third Party	44
Transmission	Phasor Measurement Unit	45
Transmission	Transmission Intelligent Electronic Device (IED)	46
Transmission	Transmission Remote Terminal Unit (RTU)	47

Source: NIST, "Guidelines for Smart Grid Cybersecurity-Volume 1," NISTIR 7628

Figure 4.2: Data-to-Framework: Design Structure Matrix of Actors and Domains

Domain	Actor	Acto	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20	21	22	23	24	25	26	2																				
Generation	Plant Control System – Distributed Control System	1	1	Generation																																											
Customer	Customer	2		2							Customer																																				
Customer	Customer Appliances and Equipment	3			3																																										
Customer	Customer Distributed Energy Resources: Generation and Storage	4				4																																									
Customer	Customer Energy Management System	5			U44	U45	5																																								
Customer	Plug-in Electric Vehicle/ Electric Vehicle Service Element	6					U62	6																																							
Customer	Home Area Network Gateway	7			U43	U130	U42	U49	7																																						
Customer	Meter	8			U120		U41		U60	8																																					
Customer	Customer Premise Display	9		U127			U126		U124		9																																				
Customer	Sub-Meter – Energy Usage Metering Device	10			U129	U48	U46	U50	Ux5	U47		10																																			
Customer	Water/Gas Metering	11							U128				11																																		
Distribution	Distribution Data Collector	12												12		Distribution																															
Distribution	Distributed Intelligence Capabilities	13													13																																
Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	15												U112	U108	15																															
Distribution	Field Crew Tools	16								U35							16																														
Distribution	Geographic Information System	17															U105	17																													
Distribution	Distribution Sensor	18												U111					18																												
Markets	Energy Market Clearinghouse	19																		19		Markets																									
Markets	Independent System Operator/Regional Transmission Organization Wholesale	20																		U17	20																											
Operations	Advanced Metering Infrastructure Headend	21							U25	U24						U3						21																Operations										
Operations	Bulk Storage Management	22																					22																									
Operations	Customer Information System	23		U125			U119										U14	U110				U21		23																								
Operations	Customer Service Representative	24		U40																				U38	24																							
Operations	Distributed Generation and Storage Management	25														U137										25																						
Operations	Distribution Engineering	26														U109											26																					
Operations	Distribution Management Systems	27					U88										U104	U102		U97		U7		U113			U114	27																				
Operations	Distribution Operator	28															U99											U101	28																			
Operations	Distribution Supervisory Control and Data Acquisition	29							U59							U117				U57						U65		U9	U100	29																		
Operations	Energy Management System	30	U74																		U72					Ux2		U87			30																	
Operations	ISO/RTO Operations	31	U70																	U58	U90		U66							U56	U89	31																
Operations	Load Management Systems/Demand Response Management System	32					U106		U32													U22		U33				U11					32															
Operations	Meter Data Management System	33																				U2						U8						33														
Operations	Metering/Billing/Utility Back Office	34							U54																					U55					34													
Operations	Outage Management System	36															U29					U26								U27						36												
Operations	Transmission SCADA	37	U80													U67							Ux3					U10		U115	U83	U116	U13				37											
Operations	Customer Portal	38		U39																				U37														38										
Operations	Wide Area Measurement System	39																													U77	U78					U75		39									
Operations	Work Management System	40															U34	U131						U31				U12					U36			U30				40								
Operations	Security/Network/System Management	48												U133				U133		U133		U133		U133	U133										U133			U133			48							
Operations	Transmission Engineering	49																																								49							
Service Provider	Aggregator/Retail Energy Provider	41					U92													U20	U93							U15		U51	U91	U52			U53						U133		41	Service Providers					
Service Provider	Billing	42								U64												U98		U96						U63		Ux6		U1	Ux4						U133		U4	42					
Service Provider	Energy Service Provider	43					U95																																		U133				43				
Service Provider	Third Party	44							U18													U6												U5							U133					44			
Transmission	Phasor Measurement Unit	45																														U134					U85		U79								45		
Transmission	Transmission Intelligent Electronic Device (IED)	46																																			U81					U135						46	
Transmission	Transmission Remote Terminal Unit (RTU)	47																																			U82					U136			Trasnsmission				47

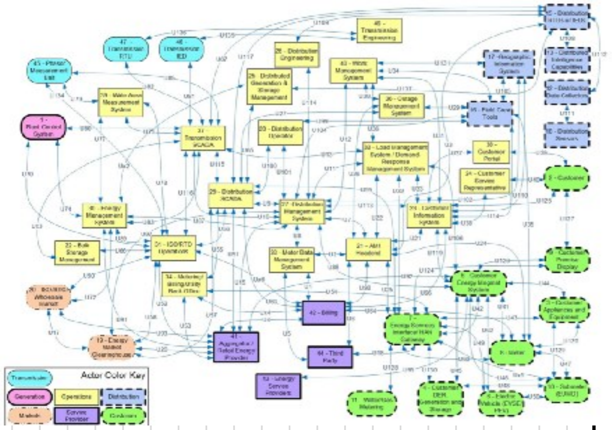


Figure 4.3: Framework to Metrics: Design Matrix Actors Domains and Logical Interfaces

4.6. From Metrics to Model

If we create the Design Structure Matrix (**Figure 4.3**), then we can generate the basic network model shown in **Figure 4.4**.

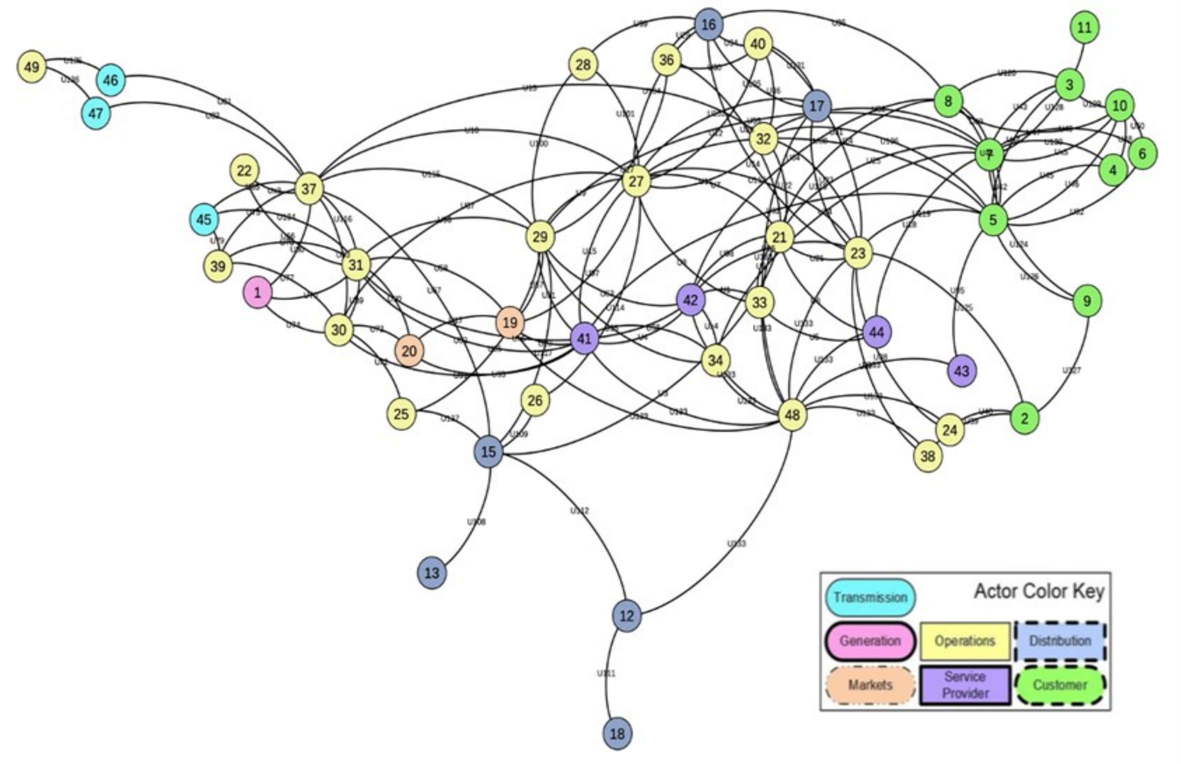


Figure 4.4: Network Basic Model

This network model is itself a data-based system. It serves as a reference case and a "laboratory" for situating, understanding, and pursuing the implementation of CSF directives, to:

- Identify and examine the implications of **C-I-A security** objectives, as well as the **Impact** levels and **Security Requirements** for nodes & logical interfaces, and
- Identify the relevant NIST Cybersecurity Framework **functions** in light of the **Impact** level.

These steps enable us to:

a. Identify critical **control points** for each node & logical interface based on the:

    i. Centrality of nodes based on logical interfaces.

    ii. Calculation & consolidation of impact scores for each C-I-A security objective.

b. Locate and consolidate **security requirements** for each C-I-A security objective, and

c. Create representations of **additional data** generated in (c) and (d) for both DSM and network views.

At this point, we transition to the impact levels of vulnerabilities and the security objectives.

4.7. Impact Levels and Security Objectives

The distribution of CSF **impact levels** and **security objectives** (C-I-A) throughout nodes and zones for the *Proof-of-Concept* network model is presented in **Figure 4.5**. Recall that the Figure derives from the DSM that is constructed from the NIST 7628 conceptual smart grid model.

This first step is of immediate relevance to the user or enterprise. It provides is a clear and specific identification of target and impact levels for each of C-I-A. Of course, the user can "drill down" or "zoom in" for further analysis.

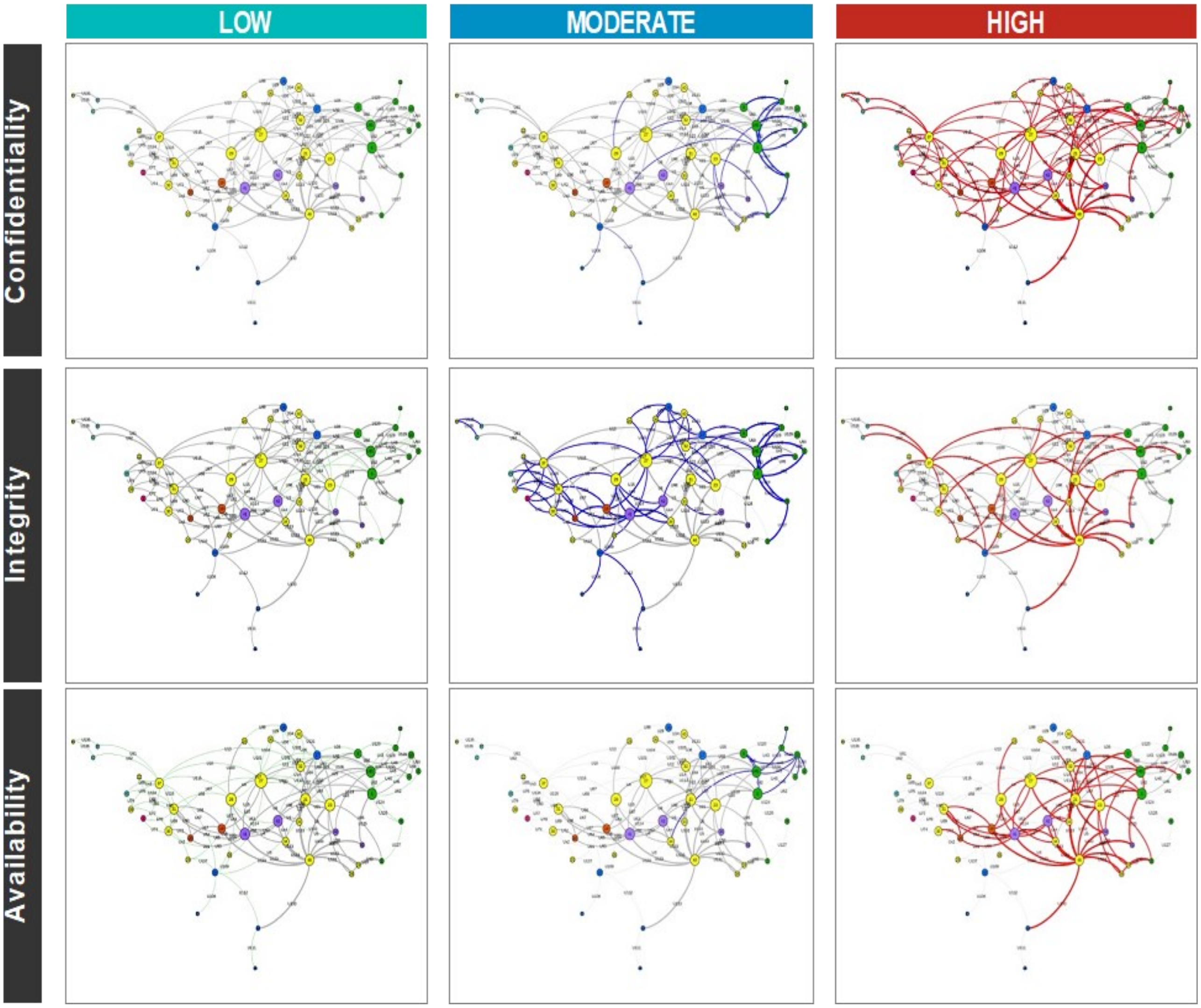


Figure 4.5: CSF Impact Levels and Security Objectives for the Network Model

Prepared by Gaurav Agarwal [aka Gaurav]

4.8. Value to the Enterprise

If an enterprise utilizes the linked database method developed in the *Proof-of-Concept* case, and seeks to customize the results to its system and operations, then it must incorporate its own enterprise specific knowledge to the structure of cybersecurity directives. In this case, it means that the enterprise must:

a. *Map its own system to the NIST "as-is" system*. Given that this work is based on a sector independent framework and guideline documents, an enterprise must map its own system components and policies to the relevant reference documents.

b. *Identify system specific vulnerabilities*. Based on the above mapping, an enterprise must also assess the threat landscape as well as the vulnerabilities identified, and/or known by the enterprise owners.

As noted earlier, every phase of the research design is based on the previous ones. This modular and cumulative approach assumes a degree of sustained validity in the database, both "raw" and "derived". If this assumption does not hold, or if there is any disruption in the validity of prior phases, then a "redo" analysis is required.

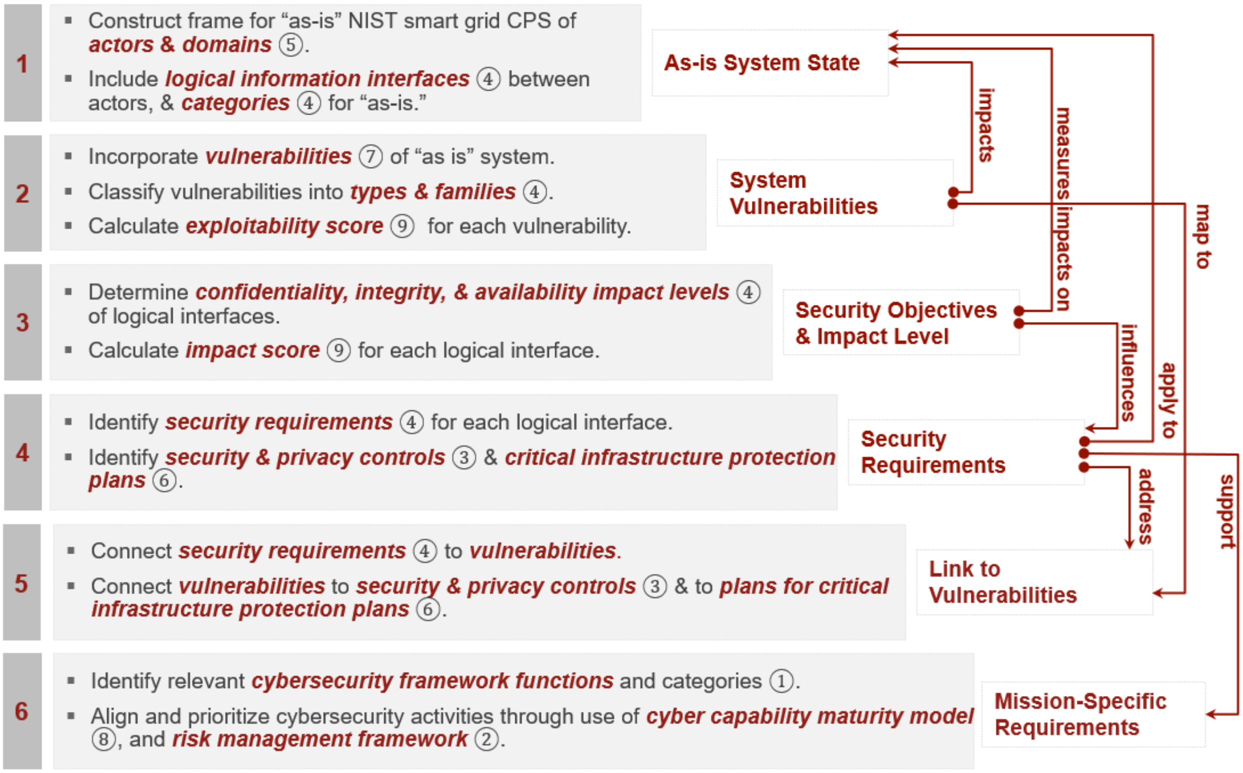
The following segment, **Section V**, addresses these issues, focusing on ***Security*** and ***Privacy***.

V. SECURITY & PRIVACY

At this point, it is useful to review the method developed so far, before we introduce a critical exogenous “disturbance” for the entire research design.

5.1. Review of the Data Linkage Process

This Section begins with a schematic representation of the data linkage process. **Figure 5.1** highlights the key features of each part of the processes – the inputs and the outputs – and points to the underlying logic thereof. This Figure is an expansion of **Table 4.1** earlier.



1
- Construct frame for “as-is” NIST smart grid CPS of ***actors & domains*** ⑤.
- Include ***logical information interfaces*** ④ between actors, & ***categories*** ④ for “as-is.”

2
- Incorporate ***vulnerabilities*** ⑦ of “as is” system.
- Classify vulnerabilities into ***types & families*** ④.
- Calculate ***exploitability score*** ⑨ for each vulnerability.

3
- Determine ***confidentiality, integrity, & availability impact levels*** ④ of logical interfaces.
- Calculate ***impact score*** ⑨ for each logical interface.

4
- Identify ***security requirements*** ④ for each logical interface.
- Identify ***security & privacy controls*** ③ & ***critical infrastructure protection plans*** ⑥.

5
- Connect ***security requirements*** ④ to ***vulnerabilities***.
- Connect ***vulnerabilities*** to ***security & privacy controls*** ③ & to ***plans for critical infrastructure protection plans*** ⑥.

6
- Identify relevant ***cybersecurity framework functions*** and categories ①.
- Align and prioritize cybersecurity activities through use of ***cyber capability maturity model*** ⑧, and ***risk management framework*** ②.

Figure 5.1: Sequence for Structured Linkage Data

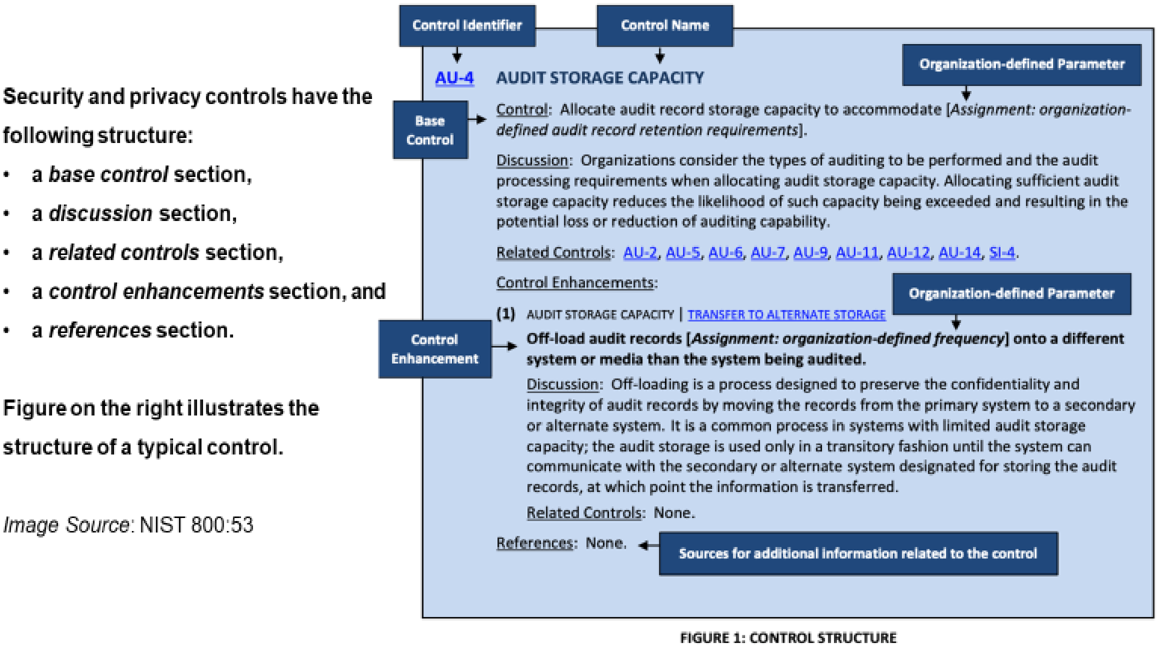
The starting point is the construction of the system “As-Is” – presented in the previous Sections – and then proceeds to incorporate the critical features of the Cybersecurity Framework, namely Confidentiality, Integrity, and Availability – and the relative impact scores.

When NIST issued a fifth revision (Rev.5) of its document 800:53, it resulted in a major disruption of sustained validity text as “raw data” for this Project.

For this project, especially important is the fact that we faced a necessary "re-do" of research steps and a review of results, with respect to:

- Data linkage process (as depicted in **Figure 5.1**),
- Information pertaining to security controls and control families,
- An unexpected entanglement between the Security and the Privacy controls, and control families, thereby creating new ambiguities,
- Data-based signals that, in the security domain, "everything is related to everything else and to privacy as well" [quotes inserted]

Given that all materials required for data linkages were provided by NIST 800:53 Rev.4, the construction of Rev.5 creates a new and entirely unforeseen imperative, namely, the *need for a "re-do" of the fundamentals for creating connections* among the diverse data sources. **Figure 5.2** shows the NIST statement on the *structure of controls*.



Security and privacy controls have the following structure:

- **a *base control* section,**
- **a *discussion* section,**
- **a *related controls* section,**
- **a *control enhancements* section, and**
- **a *references* section.**

Figure on the right illustrates the structure of a typical control.

Image Source: NIST 800:53

Control Identifier
Control Name
Organization-defined Parameter
Base Control
Organization-defined Parameter
Control Enhancement
Sources for additional information related to the control

AU-4 AUDIT STORAGE CAPACITY

Control: Allocate audit record storage capacity to accommodate [*Assignment: organization-defined audit record retention requirements*].

Discussion: Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability.

Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Control Enhancements:

(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

Off-load audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

Discussion: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary system to a secondary or alternate system. It is a common process in systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

Related Controls: None.

References: None.

FIGURE 1: CONTROL STRUCTURE

Figure 5.2: NIST Controls in 800:53 Rev.5

The "re-do" led to delineating and understanding the implications of the "entanglements" of security and privacy controls for policy implementation of the Cybersecurity Framework, or for any issues for which the use of 800:53 Rev.5 is called upon or is required.

While the “re-do” is necessitated by the fact that NIST *provided a new version of 800:53* labelled *Rev.5, the* related imperative is itself creates an added challenge, namely, to identify the differences between Rev.5 and Rev.4 for purposes of:

(a) understanding *content* and implications, and

(b) designing and implementing a *“re-do” strategy*.

With the above operational challenge, we can then construct the DSM with the NIST 800:53 Rev 5 – a critical repeat task.

5.2. “Re-Do” Results – Rev.5

The entire control system and structure of NIST 800:53 Rev.5. is shown in **Figures 5.3**. The overarching feature is the entanglements, interconnections, and density of controls – spanning both security controls and privacy controls.

Figure 5.4 situates the privacy controls in the overall system of control. The overlapping controls and interconnections are not easy to discern in these overarching network views.

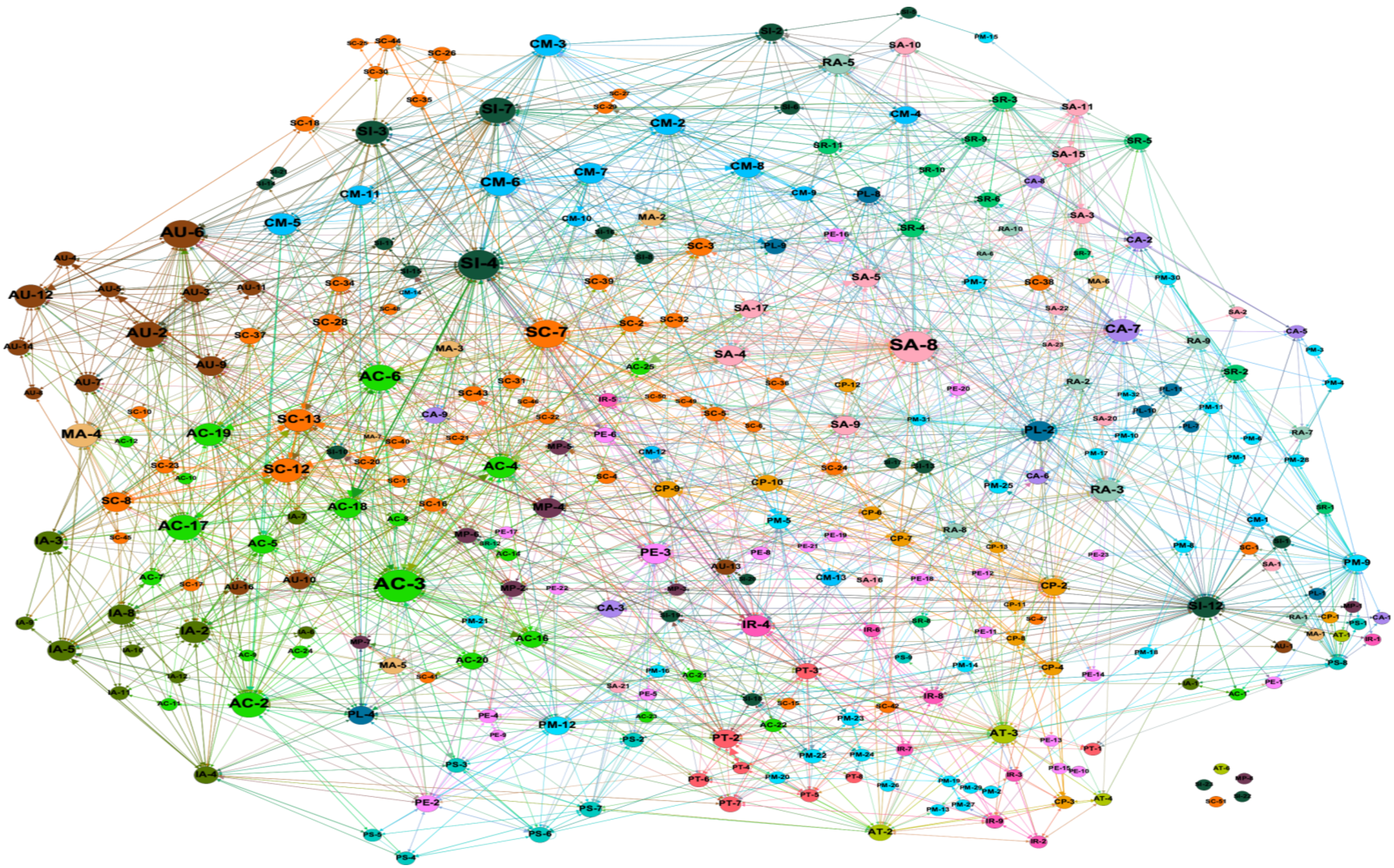


Figure 5.3: Computed Network View of NIST 800:53 System of Controls: Interconnections of Privacy and Security controls. Based on DSM prepared by Gaurav Agarwal [aka Gaurav]

Based on current and new controls, and enhancements. Not included are controls and enhancements withdrawn in Rev.4 and/or Rev.5. This graph only shows the controls, with enhancements aggregated at the control level. Node *color* indicates control family. Node *size* indicates node eigen-centrality.

Operationally, the major task in the “re-do” involves the use of 800:53 Rev.5 Design Structure, for data linkage purposes in order to create the basic network model. *This is the one document that provides the connection across the “re-do” activities required.* The initial results – *yet to be fully validated* –indicate that both privacy and security controls appear to be *heavily interdependent*.

The new results for Rev.5 are *very different* from the results of Rev.4, where privacy controls are added (in “band-aid” form) as an annex to the document. This “re-do” is also essential for the work on “reversing the arrows” in **Figure 5.1** above, i.e., starting from the last step and working “backward” to the first step. This initiative is a new segment of the research design developed for two reasons:

First, as a validation check of the process developed for the *Proof-of-Concept,* and

Second, as a means of providing alternative ways for addressing core linkage issues.

In other works, if the method we have developed “works one way,” let us figure out if it “works, the other way as well.”

5.3. NIST Mission for Rev.5

Revision 5 of this foundational publication, NIST 800.53, represents a multi-year effort to develop the next generation for security and privacy controls that will be needed to accomplish the above objectives. It includes changes to make the controls more usable by diverse consumers groups (e.g., enterprises conducting mission and business functions; engineering organizations developing information systems, IoT devices, and systems-of-systems; and industry partners building system components products, and services.)

The most significant changes to this publication include:

- Making controls more outcome-based by removing the entity responsible for satisfying the control (i.e., information system, organization) from the control statement;
- Integrating information security and privacy controls into a seamless, consolidated control catalog for information systems and organization; Establishing a new supply chain risk management control family;
- Separating control selection processes from the controls, thereby allowing the controls to be used by different communities of interest, including systems engineers, security architects, software developers, enterprise architects, systems security and privacy engineers, and mission or business owns.

Rev.5 affected all earlier work in this Project with respect to:

- Data linkage process
- Information pertaining to security controls and control families

In addition, Rev.5 demonstrates:

- An unexpected entanglement between the Security and the Privacy controls, and control families, thereby creating new ambiguities.

And creates:

- Data-based signals that, for security and privacy purposes, everything is related to everything else.

We noted earlier that the “re-do” creates new tasks in the research design, and involves completion of several research items that are additions to the workplan. These additions involve:

(a) providing added validation to the process,

(b) expanding the domain uses of our research, and

(c) creating value-added for the use of the Cybersecurity Framework (CSF).

The next segment of this Compilation, **Section VI**, turns to fundamental issues in this research initiative.

V. SECURITY & PRIVACY: References

1. National Institute of Standard and Technology (NIST). (September 2020) NIST SP 800-53, Rev.5 Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

VI. RESEARCH FUNDAMENTALS

Our first-order applications of method-development and testing concentrate on one complex pervasive cyber-physical system, namely, the smart grid for electric power systems. However, the problems addressed are generic in form, and the methods we have developed have wide-ranging applications.

6.1. NIST as "Laboratory"

Of the many powerful contributions provided by NIST over the years, we find its role as a "laboratory' to be extremely important and understated. As such, the specific features of this "laboratory" serve well as a "test-bed" for the *Proof-of-Concept* case focusing on cybersecurity policy of a smart grid as a cyber-physical system.

The *Proof-of-Concept* draws entirely on the conceptual model developed by NIST and on related NIST directives and documents. This case analysis is selected because of:

a) Smart grid **salience** throughout the industry and society,

b) **Complexity** as a *cyber-physical* system, and the opportunity to build on the extensive work done by NIST,

c) Excellence as a domain of research on **analytics** for cybersecurity policy of cyber-physical systems, and

d) Importance for "**NIST as a Laboratory.**"

The policy complex is the *Cybersecurity Framework (CSF)* **[1]**, including its directives. As noted, CSF is mandatory in the public sector and greatly encouraged for the private sector. CSF directives provide tools to enable policy implementation. However, the *mission-specific* or *industry-specific* application is left to the user—with only general guidance provided by CSF directives.

NIST as "Laboratory" enables us to:

a) develop analytics for cybersecurity policies and guidelines,

b) assist in understanding the full implications of the guidelines, and

c) provide methods to facilitate use of CSF in diverse contexts and applications.

In addition to Project **analytics**, we developed **practical** uses for making it easier to use the Cybersecurity Framework.

6.2. Practical Uses

Here we signal four practical uses of research and results so far:

6.2.1. *Data Linkages*

One: The full value of CSF is difficult to capture given the set of intervening tasks required and the distributed nature of the database. CSF points to ***what*** has to be done and ***why,*** but ***not how.*** It is up to the user to work through the process outlined by CSF. Pointers to steer users to other documents are provided.

In this case, the practical use is created by providing a **method to streamline** access to, and use of, essential data required to implement the security-related actions required by CSF. Because CSF points to a number of individual documents hosting different directives, the users' task is to identify and make connections among them as needed.

Moreover, modifications and updates by NIST on the content of key intervening documents require users, in turn, to0 identify the updates, and to determine requirements for change.

6.2.2. *Metrics & Measures*

Two: Given that policy documents and directives are conveyed in text form – in linear sequential order – it is common practice to retain information in that form alone. We developed a method to transform text into metrics so that we can to deal with numerals as well not just letters.

The practical use is compelling: **metrics and measures** enable more precision, with more flexibility in scale and scope of analysis, than can ever be done with the text form. This in itself takes away much of the built-in ambiguity of policy documents. Since the method is portable, it can be applied to all forms of policy texts – irrespective of issue area or domain.

6.2.3. *Models & Network Analysis*

Three: The reference model for the NIST Smart Grid as a cyber physical system is notable. This model is derived from the metrics and measures embedded in the Design Structure Matrix (DSM) representation of the descriptive text for the NIST Conceptual or Reference Model of smart grid as an example.

Unexpected and **exogenous disruptions** of data-at-the-source, noted earlier, created the need to **"re-do"** research steps previously completed. In such cases, revision is a necessity not a choice.

6.2.4. *Updates and Value Added*

Four: The fifth revision (Rev.5) of NIST 800:53, provides new formal connections, or interfaces, between multiple sources of "raw" data central to the *Proof-of-Concept.*

In addition, Rev.5 couples very closely the ***controls*** and ***control families*** to security and privacy. As such, Rev.5 also raised important question about the implications of this new version of 800:53, in terms of current NIST perspectives and priorities pertaining to security. Such a reassessment is essential for understanding changes in the overall policy landscape for cybersecurity policy of cyber-physical systems.

6.3. Security and Privacy

More specifically, 800:53 Rev.5 is called upon or required. Rev.5 affects all earlier analyses with respect to:

- Data linkage process
- Information on security controls and control families

In addition, Rev.5 demonstrates:

- An unexpected entanglement between the Security and the Privacy controls, and control families, thereby creating new challenges, even ambiguities,

And creates:

- Data-based signals that, for security and privacy purposes, “everything is related to everything else”.

We noted earlier that the “re-do” created **additions** to the research design. The empirical research design is augmented by:

(a) providing added validation to the process,

(b) expanding the domain uses of our research, and

(c) creating value-added for the use of the Cybersecurity Framework (CSF).

As noted, the “re-do” addresses serious challenges to the “reversing the arrows” principle and to the first-order validation strategy for our research design.

The most notable challenge pertains to the process of *from* the user final-requirement and *back up* the chain of sequence to the “As-Is” system model. By necessity, that situation requires the use of 800:53 Rev.5 and adapted to the reversal of the sequence shown in **Figure 5.1** earlier.

Recall that constructing the DSM is critical for *transforming text into metrics*. By necessity, we *re-construct* the DSM with the NIST 800:53 Rev.5.

6.4. Policy Analytics in Parts

It should be evident by now that one Part of the research design focuses on analytics for the **cyber-physical system** itself. Another Part is on analytics for cybersecurity **policies and directives.**

Both Parts share a common process that must be applied to each side separately because the data are distinct. Here we review and we simplify the process of Text-to-Model.

- **Text to Data**
- **Data to Metrics**
- **Metrics to Model**

Part I generates the *proof-of-concept* model that provides the platform or system that is linked to Part II.

Part II identifies empirically the logical interfaces for the system "As Is" that, in turn, connect to CSF directives. These directives consist of:

i. ***Impact levels*** for each Confidentiality, Integrity, and Availability security objective (C-I-A),

ii. ***Vulnerability*** levels in terms of impact,

iii. ***Security Requirements*** based on Impact level for each C-I-A security objective,

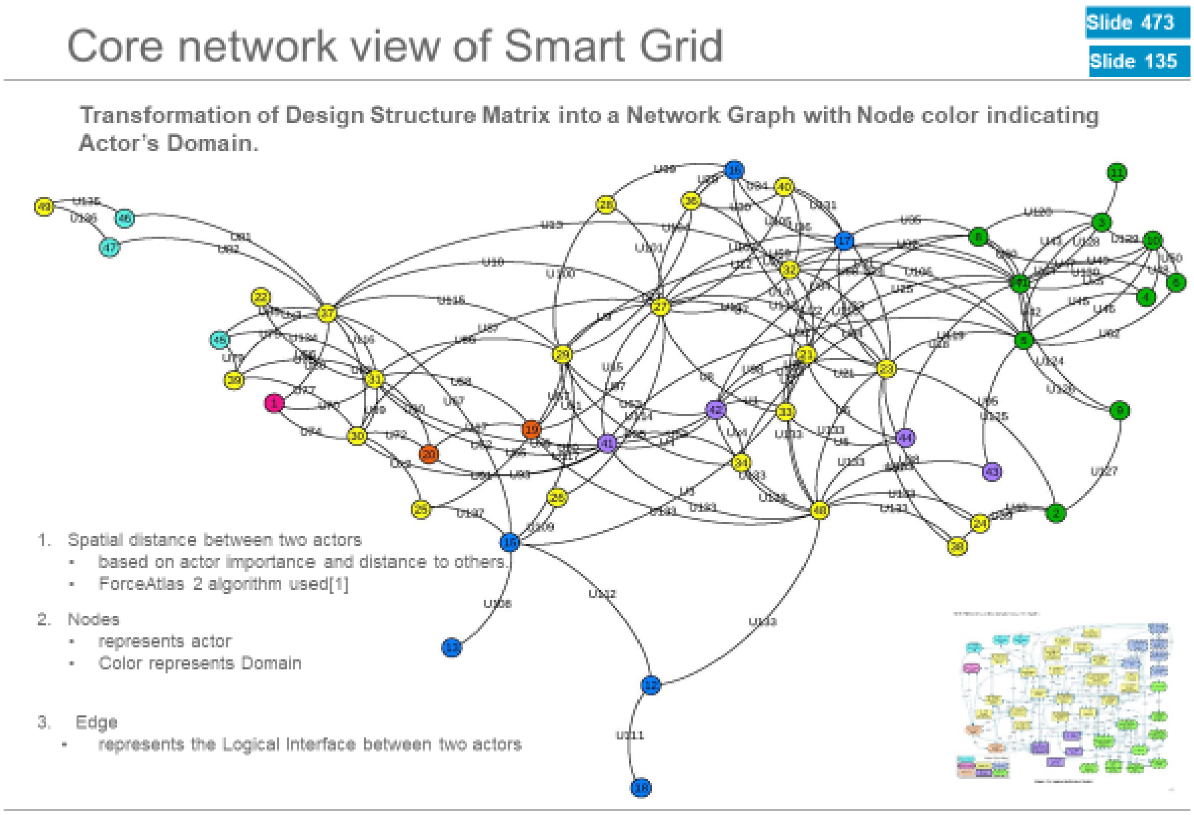
iv. ***CSF functions*** based on Impact level.

Part III pertains to connectivity. And this brings us to the next challenge.

6.5. Linking the Parts

The major task in the "re-do" involves testing and re-testing the construction of the Design Structure Matrix (DSM) with 800:53 Rev.5. This is the one document that provides the connection across the "re-do" activities required.

The result is displayed in **Figure 6.1**. The basic network model shows an individual actor represented by a node; and the logical interface between any two actors is an edge between the two actors. This Figure presents an actor-neutral view, so to speak, to demonstrate the overall system architecture and to serve as the reference case.



Core network view of Smart Grid

Slide 473
Slide 135

Transformation of Design Structure Matrix into a Network Graph with Node color indicating Actor's Domain.

1. Spatial distance between two actors
   - based on actor importance and distance to others.
   - ForceAtlas 2 algorithm used[1]
2. Nodes
   - represents actor
   - Color represents Domain
3. Edge
   - represents the Logical Interface between two actors

Figure 6.1: Network Model - Basic Reference Case

The “re-do” process, requires us to identify the differences between Rev.5 and Rev.4 for purposes of:

a) Understanding the ***content*** and ***implications*** of the *“re-do”*

b) Establishing the **new connection** between the Parts.

The “re-do” enables us to proceed with confidence, and:

c) Identify critical ***control points*** for each node and logical interface based on the:

   a. ***Centrality*** of nodes based on logical interfaces.

   b. ***Calculation and consolidation*** of impact scores for each C-I-A security objective.

d) Situate and consolidate ***security requirements*** for each C-I-A security objective.

e) Create ***representations*** of additional data generated in (c) and (d) for both DSM and network views.

The validated “re-do” shows a clear result, noted earlier, namely that privacy and security controls are *heavily dependent on each other, thus creating “noise” in the focused analysis of security controls.*

6.6. High Salience Network View

The network model in **Figure 6.2**, based on the DSM, is generated by ForceAtlas logic algorithm of Gephi 0.9.2 software **[2] [3]**. Here the use of this algorithm produces a spatially structured network, where nodes repulse each other, akin to charged particles, while edges attract their nodes, like springs. Jointly they converge to a balanced state.

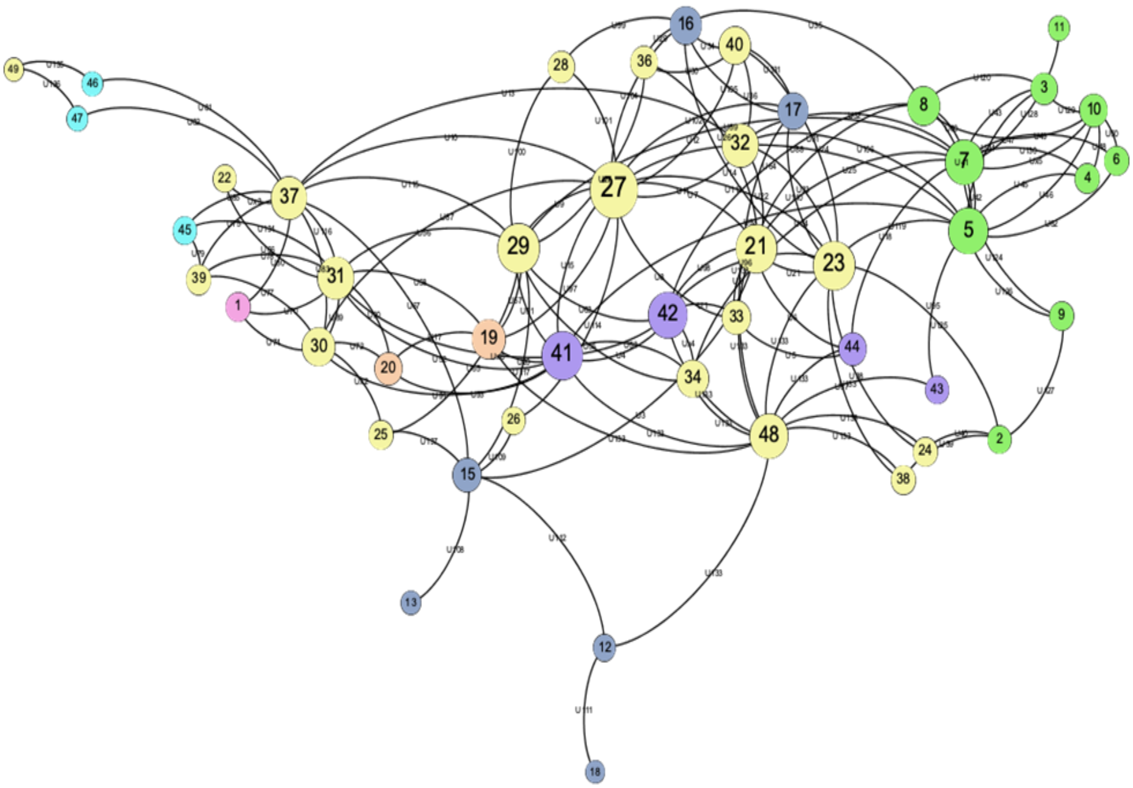


Figure 6.2: Eigenvector centrality-view of actors in Reference Model

Source: Derived from Design Structure Matrix in **Figure 4.3**

Operationally, this process situates each node based on the location of other nodes, and depends only on the connection between nodes. Here, the position of a node cannot be defined on its own; it can be determined only when compared to the others in the system.

Figure 6.3 lists the rules with the greatest centrality distilled from the system-wide view in **Figure 6.2** above. For convenience we also identify each rule and chapter.

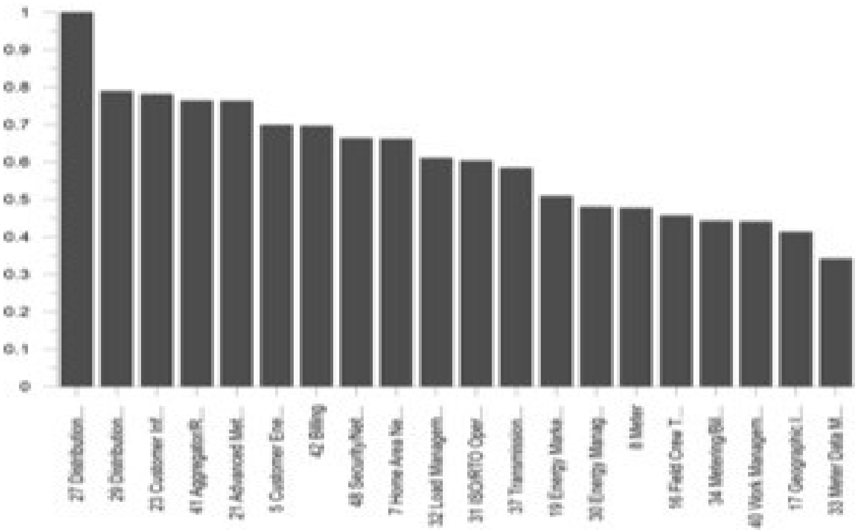


Figure 6.3 Actors in system model with highest Eigenvector centrality

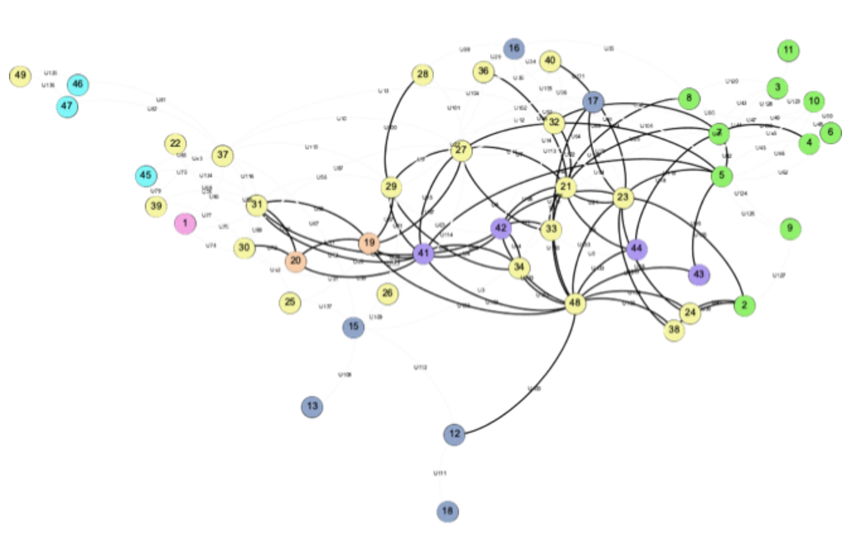
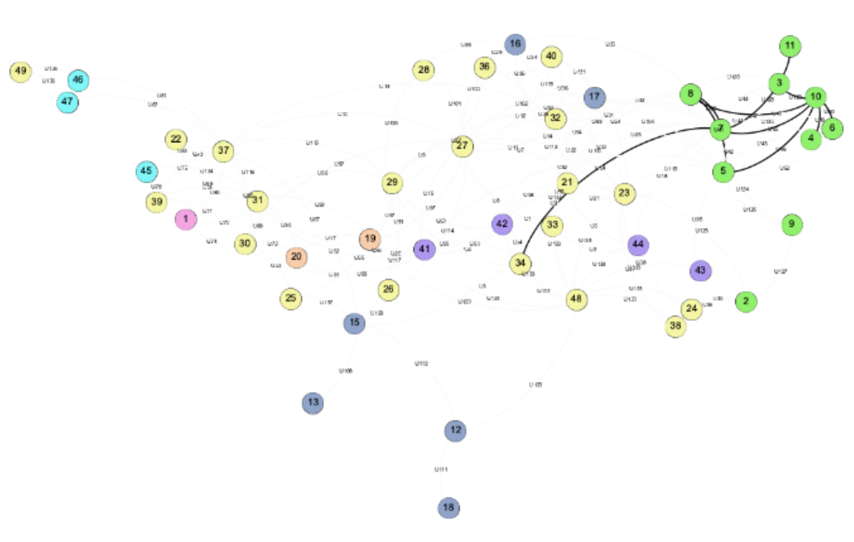
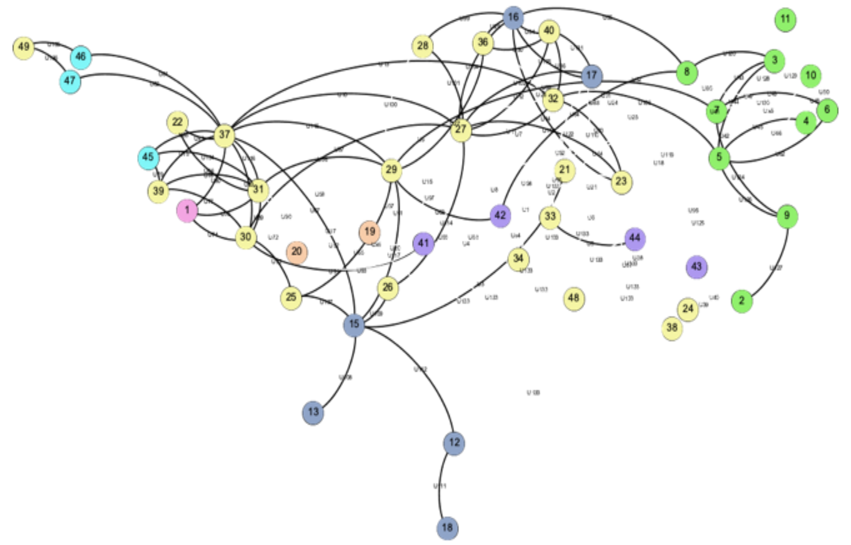
Source: Derived from **Figure 6.2**

Further, NISTIR provides the **impact level** on a logical interface category for each of the three security objectives. This information is transferred to a logical interface. This is then followed by an aggregation to the for highest impact level if a logical interface belongs to more than one category.

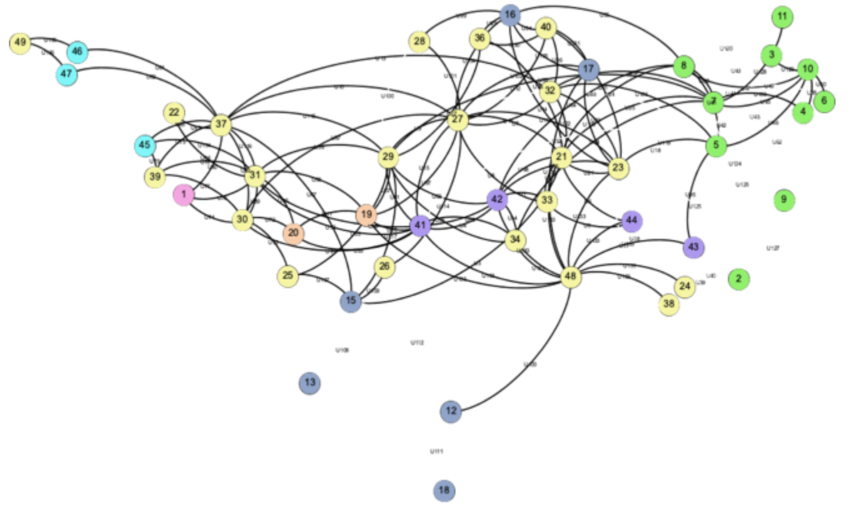
Figures 6.4a – 6.4c show the results for each of the C-I-A security objectives. And **Figure 6.5** is an aggregation, a summary of the results for the three security objectives. As a re minder, in these Figures the following holds:

- Node represents an **actor**
- Node color represents the **domain** to which the actor belongs
- Node size represents the **centrality** of the node.
- Edge represents the **logical interface** connecting the two actors.
- Edge **color** {Green, Orange, Red} represents the **impact level** {Low, Moderate, High} respectively on a logical interface.

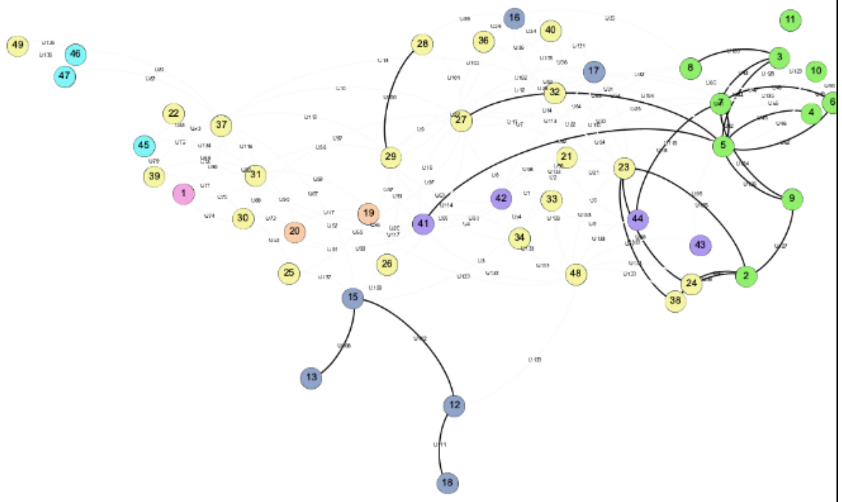
Brief inferences are appended to each Figure to assist in highlighting elements of relevance.

Logical Interfaces with High Impact	**Logical Interfaces with Moderate Impact**
	
Logical Interfaces with Low Impact	
	**Figure 6.4a: Network Model – Identifying impact level for Confidentiality security objective** Note the paucity of moderate impact, and the salience of low impact.

Logical Interfaces with High Impact



Logical Interfaces with Moderate Impact



Logical Interfaces with Low Impact

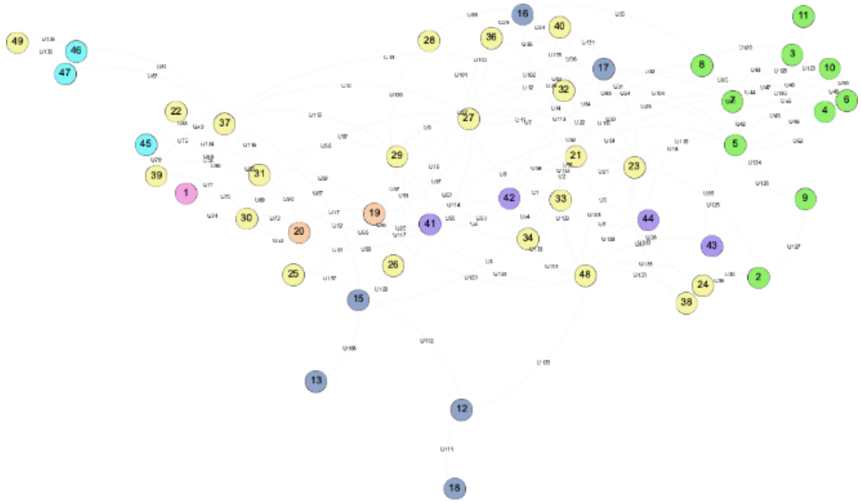
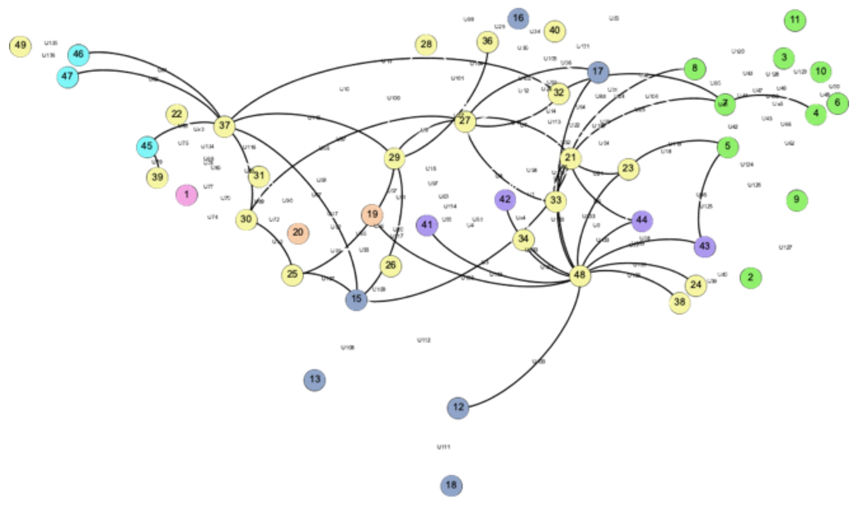


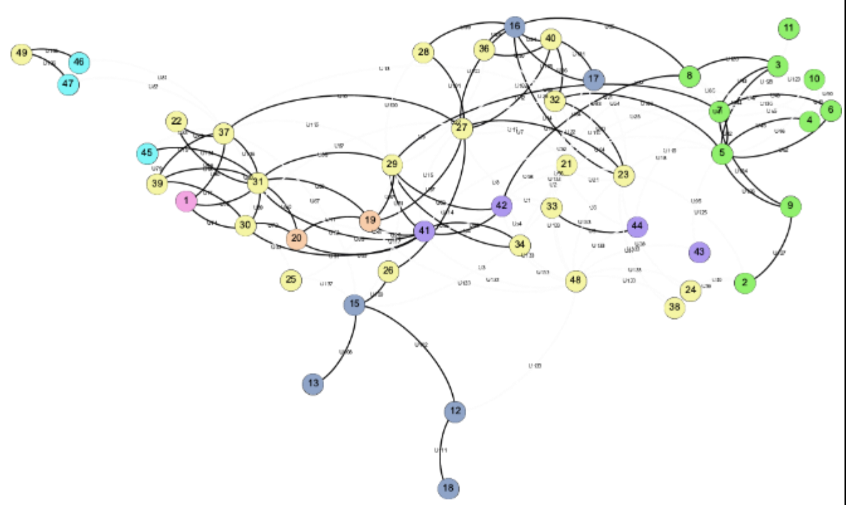
Figure 6.4b: Network Model – Identifying impact level for <u>Integrity</u> security objective

Logical interfaces with high impact are dominant throughout the entire system – with the exception of several interfaces with moderate impact. The absence of low impact interfaces is noteworthy.

Logical Interfaces with High Impact



Logical Interfaces with Moderate Impact



Logical Interfaces with Low Impact

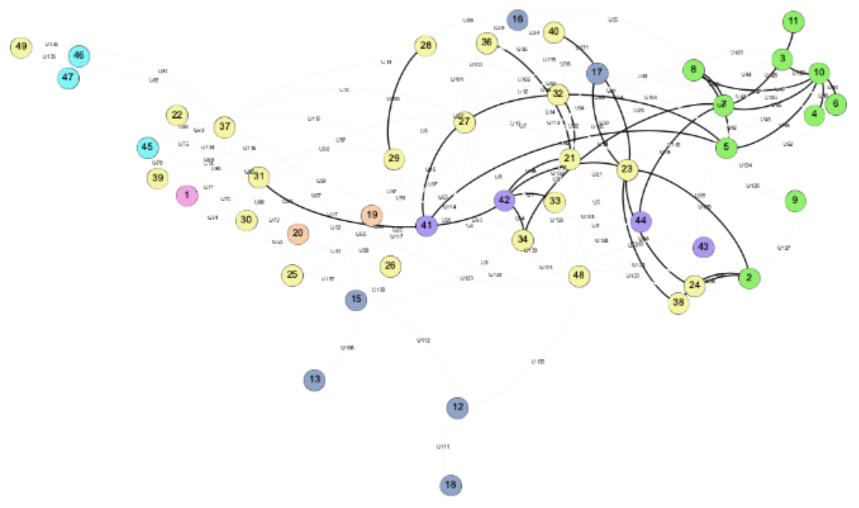
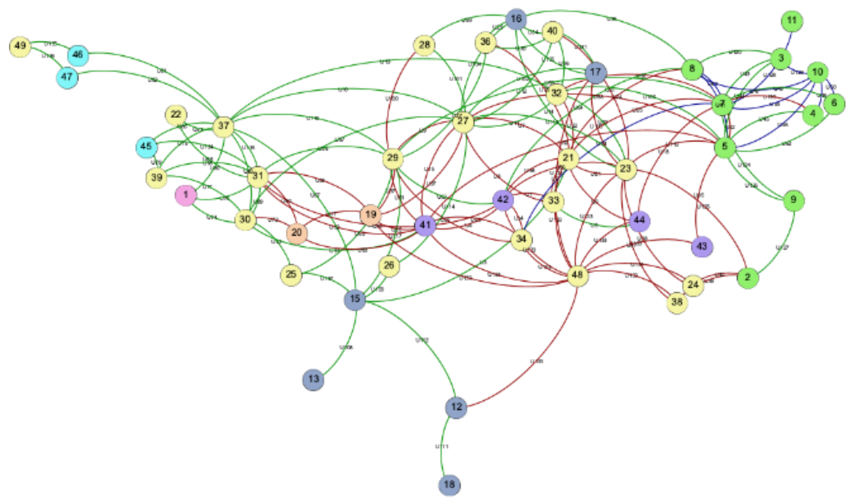
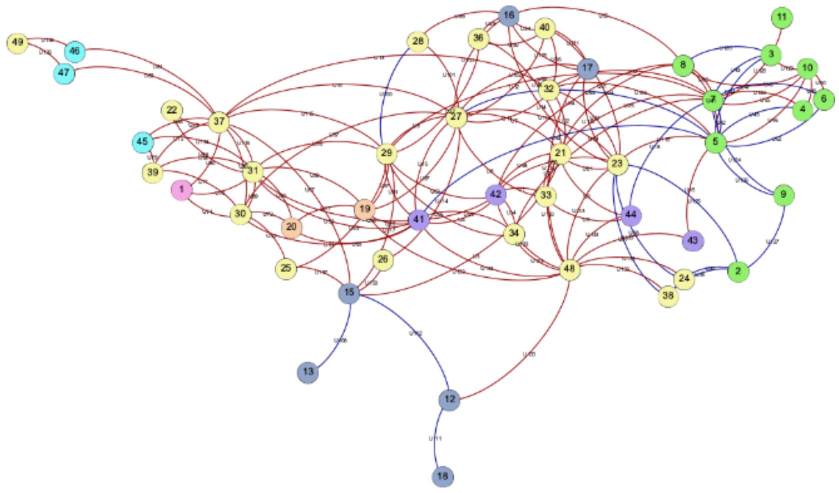
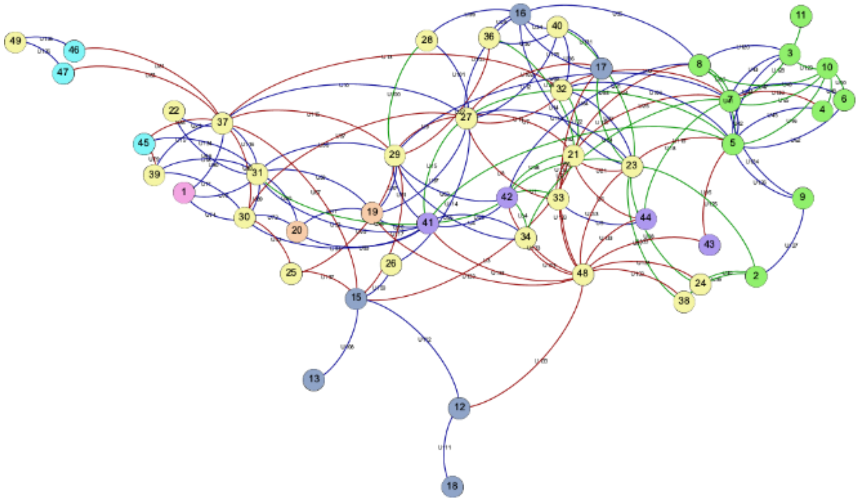


Figure 6.4c: Network Model – Identifying impact level for <u>Availability</u> security objective

High and moderate impact levels are more apparent than low impact interfaces.

Confidentiality	**Integrity**
	
Availability	
	**Figure 6.5: Network Model – Summary of Impact Level** *Source: Aggregated from Figures 6.4a -6.4c* The summary impact levels appear to override any distinctions apparent at the individual C-I-A requirement. Prepared by Gaurav Agarwal [aka Gaurav]

VI. RESEARCH FUNDAMENTALS: References

1. National Institute of Standards, and Technology. Framework for improving critical infrastructure cybersecurity. 2014. https://www.nist.gov/cyberframework

2. M. Bastian, S. Heymann and M. Jacomy, "Gephi: an Open Source Software for Exploring Manipulating Networks", Association for the Advancement of Artificial Intelligence. 2009.

3. Jacomy M, Venturini T, Heymann S, Bastian M (2014) “ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software”. PLOS ONE 9(6): e98679. https://doi.org/10.1371/journal.pone.0098679

VII. INTEGRATED VULNERANILITY IMPACTS

Missing so far is a **net assessment of vulnerability impacts** for the logical interfaces across three dimensions and three levels of intensity. We now turn to the consolidation and integration of impact analysis. The task is to generate one net vulnerability score based on *Common Vulnerability Scoring System* (CVSS).

7.1. Toward Consolidated System Vulnerability Impacts

CVSS provides a way to capture the principal characteristics of a vulnerability. It is an open framework for communicating the characteristics and severity of system vulnerabilities. CVSS produces a numerical score—ranging from 0 to 10—reflecting its severity based on:

- **Impact metrics**—based on Confidentiality Impact, Integrity Impact, Availability Impact—on reflect the direct consequence of a successful exploit and represent the consequence to the target that suffers the impact.

- **Exploitability metrics** reflect the ease and technical means by which the vulnerability can be exploited.

Figure 7.1 shows the consolidation of analysis and results in **Figure 6.5** for Impact levels of system vulnerabilities into one integrated system view, with all nodes as "equal."

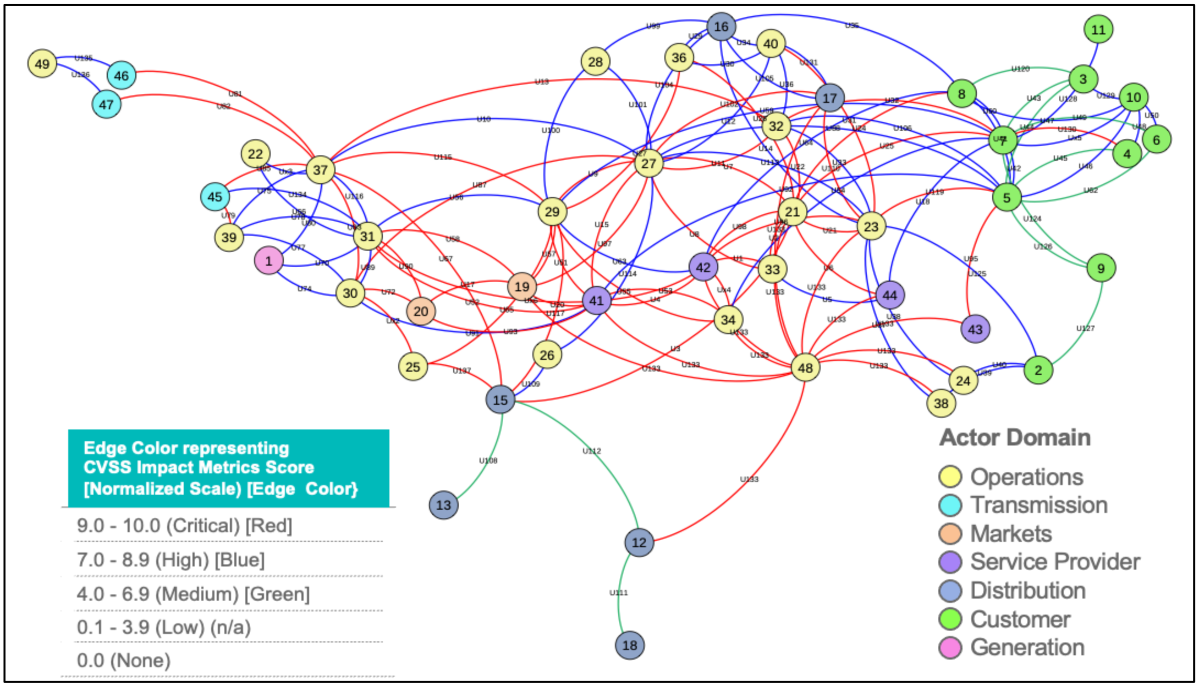


Figure 7.1: Proof-of-Concept: NIST Smart Grid: Edge impact level based on CVSS 3.0

Figure 7.2 shows the centrality or salience metric for each node in the *Proof-of-Concept* – that is the NIST conceptual model of smart grid electric power system.

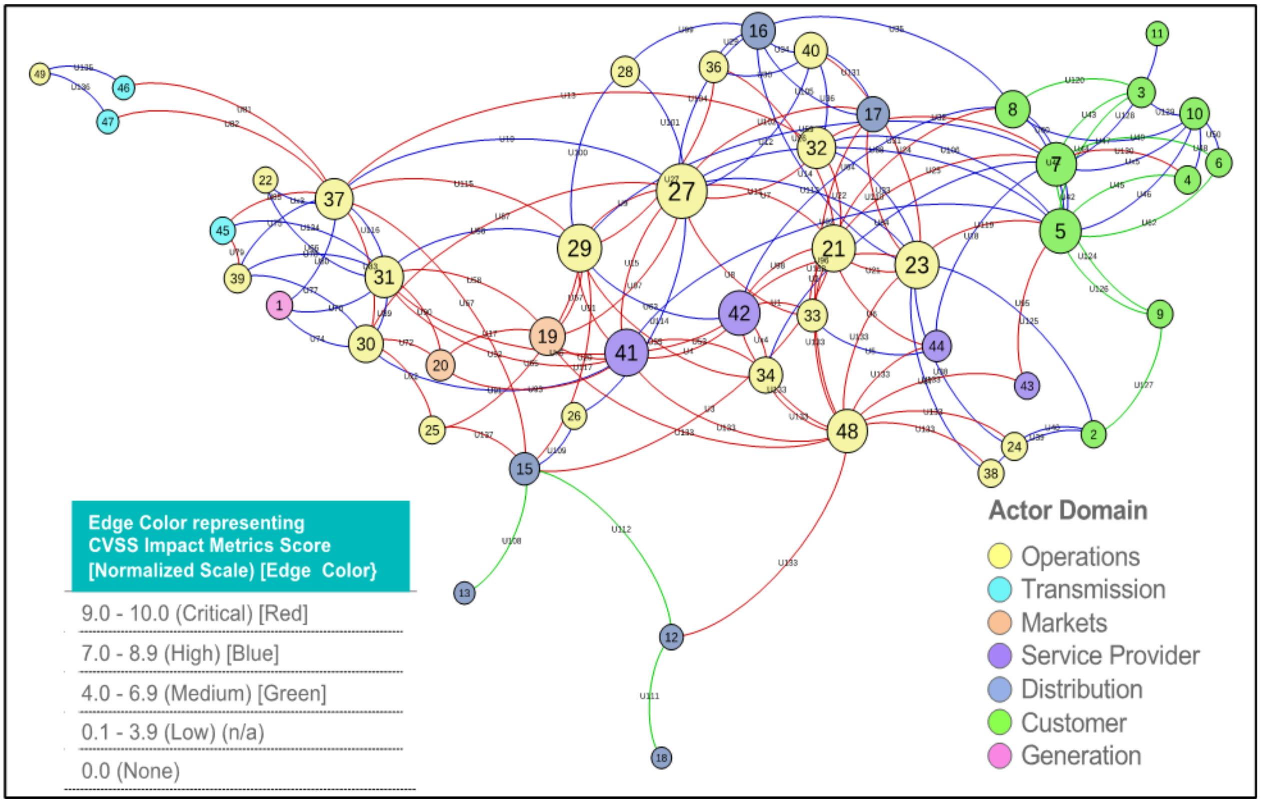


Figure 7.2: Proof-of-Concept: NIST network model edges impact level based on CVSS 3.0
Prepared by Gaurav Agarwal [aka Gaurav]

The differences among node-salience in the system as a whole may be of greater relevance to user or operator – depending on defined goals.

7.2. Assessment of security requirements for logical interfaces

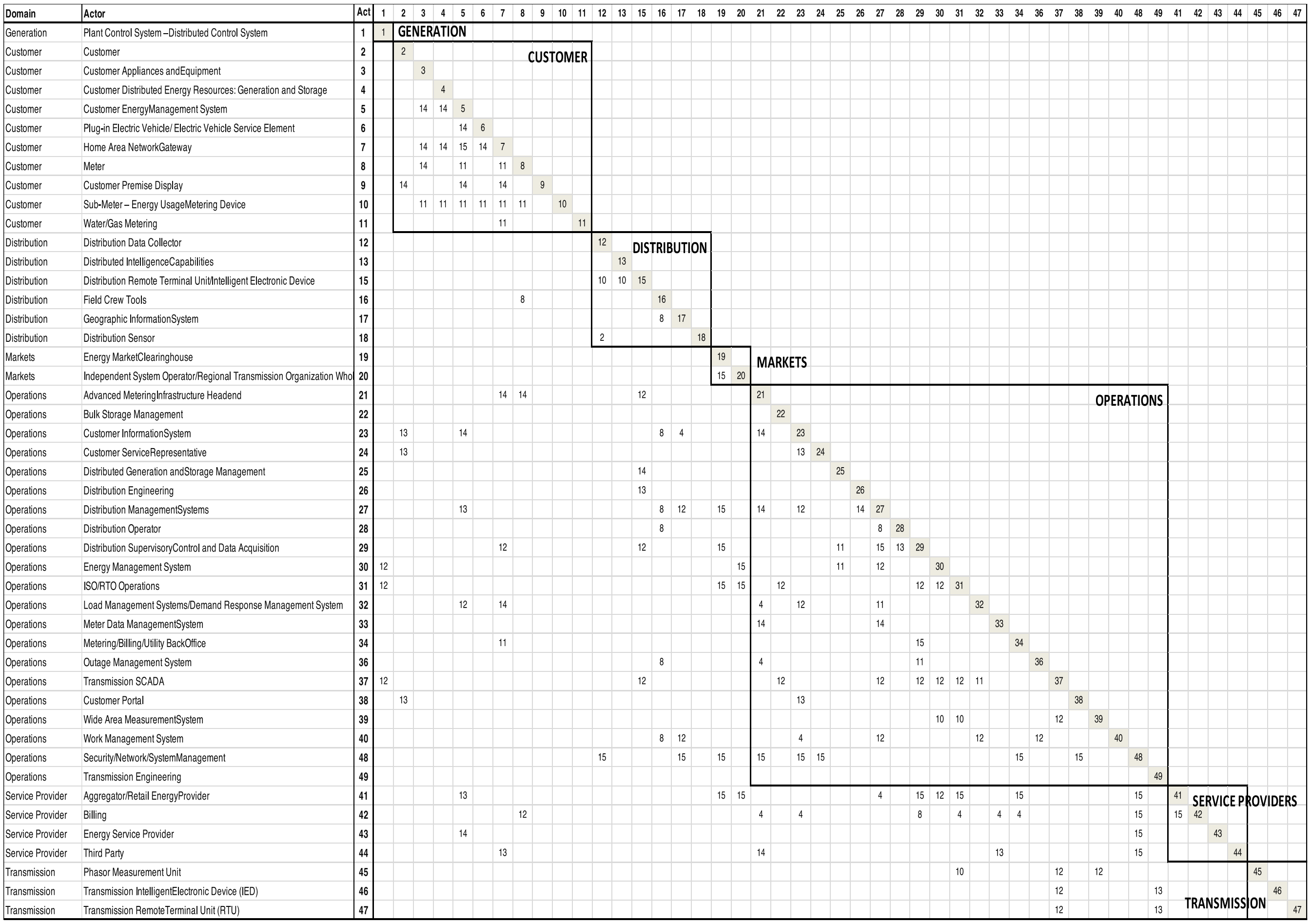
The focus now is on security requirements as stated in NISTIR 7628 (item ④ in **Figure 3.5**) that are derived from NIST SP 800:53 (item ② also in **Figure 3.5**. These security requirements are categorized into three types:

1. **Governance Risk and Compliance:** The intent is to address challenges at the organization level. GRC requirements, while centered around policy, procedure, and compliance-based activities, may include technical implications. It may be necessary to augment these organization-level requirements for different types of organizational security structures, specific logical interface categories, and/or smart grid information systems.

2. **Common Technical Requirements:** The common technical requirements are applicable to all of the logical interface categories.

3. **Unique Technical Requirements:** The unique technical requirements are allocated to one or more of the logical interface categories.

Figure 7.3 aggregates the count of unique security requirement for each logical interface in a DSM format.



GENERATION
CUSTOMER
DISTRIBUTION
MARKETS
OPERATIONS
SERVICE PROVIDERS
TRANSMISSION

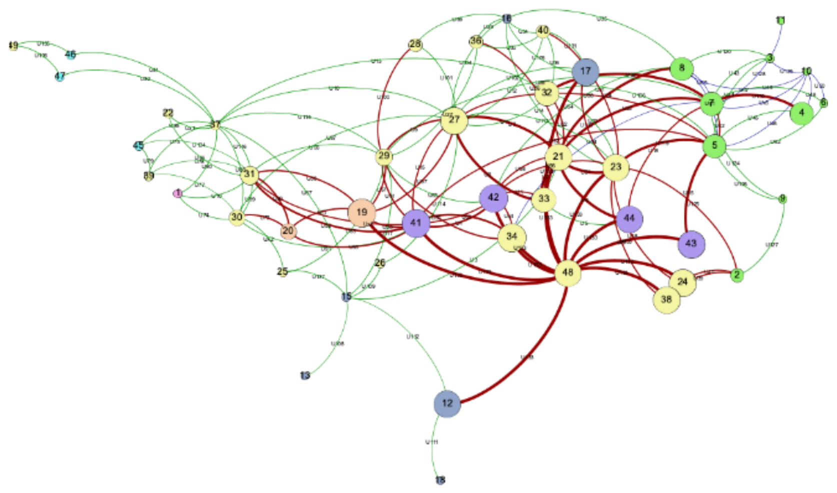
Domain	Actor	Act	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	36	37	38	39	40	48	49	41	42	43	44	45	46	47
Generation	Plant Control System –Distributed Control System	1	1																																														
Customer	Customer	2		2																																													
Customer	Customer Appliances andEquipment	3			3																																												
Customer	Customer Distributed Energy Resources: Generation and Storage	4				4																																											
Customer	Customer EnergyManagement System	5			14	14	5																																											
Customer	Plug-in Electric Vehicle/ Electric Vehicle Service Element	6					14	6																																										
Customer	Home Area NetworkGateway	7			14	14	15	14	7																																									
Customer	Meter	8			14		11		11	8																																								
Customer	Customer Premise Display	9		14			14		14		9																																							
Customer	Sub-Meter – Energy UsageMetering Device	10			11	11	11	11	11	11		10																																					
Customer	Water/Gas Metering	11							11				11																																			
Distribution	Distribution Data Collector	12												12																																		
Distribution	Distributed IntelligenceCapabilities	13													13																																	
Distribution	Distribution Remote Terminal Unit/Intelligent Electronic Device	15												10	10	15																																
Distribution	Field Crew Tools	16								8							16																															
Distribution	Geographic InformationSystem	17															8	17																														
Distribution	Distribution Sensor	18												2					18																													
Markets	Energy MarketClearinghouse	19																		19																												
Markets	Independent System Operator/Regional Transmission Organization Whol	20																		15	20																											
Operations	Advanced MeteringInfrastructure Headend	21							14	14							12						21																										
Operations	Bulk Storage Management	22																					22																									
Operations	Customer InformationSystem	23		13			14										8	4				14		23																								
Operations	Customer ServiceRepresentative	24		13																				13	24																							
Operations	Distributed Generation andStorage Management	25														14										25																						
Operations	Distribution Engineering	26														13											26																					
Operations	Distribution ManagementSystems	27					13										8	12		15		14		12			14	27																				
Operations	Distribution Operator	28															8											8	28																			
Operations	Distribution SupervisoryControl and Data Acquisition	29							12							12				15						11		15	13	29																		
Operations	Energy Management System	30	12																			15					11		12			30																	
Operations	ISO/RTO Operations	31	12																		15	15		12							12	12	31																
Operations	Load Management Systems/Demand Response Management System	32					12		14													4		12				11						32															
Operations	Meter Data ManagementSystem	33																				14						14							33														
Operations	Metering/Billing/Utility BackOffice	34							11																						15						34													
Operations	Outage Management System	36																8					4								11								36												
Operations	Transmission SCADA	37	12														12							12					12		12	12	12	11				37											
Operations	Customer Portal	38		13																				13															38										
Operations	Wide Area MeasurementSystem	39																													10	10					12		39									
Operations	Work Management System	40															8	12						4				12					12			12				40								
Operations	Security/Network/SystemManagement	48												15				15		15		15		15	15										15			15			48							
Operations	Transmission Engineering	49																																									49						
Service Provider	Aggregator/Retail EnergyProvider	41					13													15	15							4		15	12	15			15						15		41						
Service Provider	Billing	42								12												4		4						8		4		4	4						15		15	42					
Service Provider	Energy Service Provider	43					14																																		15				43				
Service Provider	Third Party	44							13														14												13							15					44			
Transmission	Phasor Measurement Unit	45																															10					12		12										45		
Transmission	Transmission IntelligentElectronic Device (IED)	46																																					12					13						46	
Transmission	Transmission RemoteTerminal Unit (RTU)	47																																					12					13							47

Figure 7.3 DSM of aggregated for unique technical security requirements of all security objective, applicable on a logical interface category

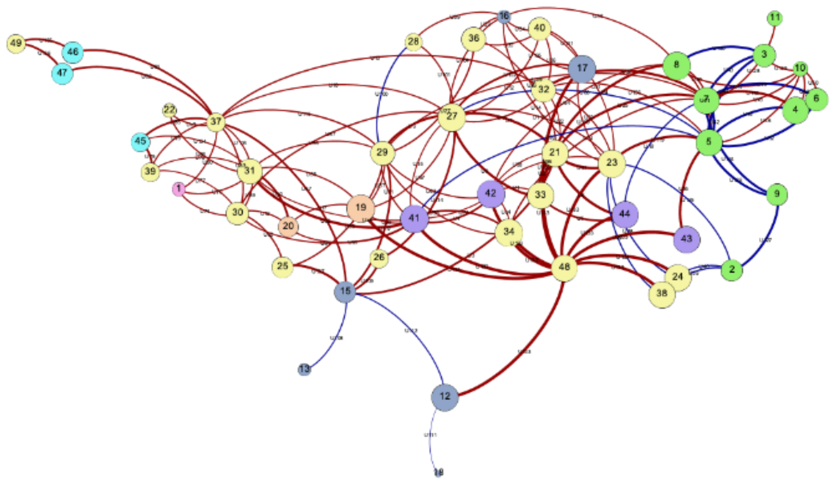
Figure 7.4 shows the aggregated count of unique technical security requirements, for all security objectives, applicable on a logical interface category. These views are derived from the DSM in **Figure 7.3**.

The next segment, **Section VIII,** highlights key elements of a protocol for cybersecurity policy analytics of cyber-physical systems.

Confidentiality



Integrity



Availability

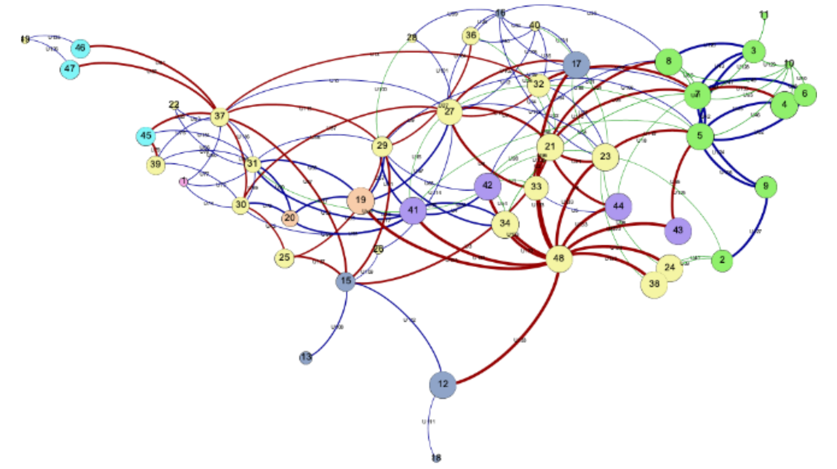


Figure 7.4: Aggregated count of unique technical security requirements for all security objective, applicable on a logical interface category
Source: Based on Figure 7.3

Note the system-wide similarity of Integrity and Availability for aggregated count of unique technical security requirements, for all security objectives, on a logical interface category.
Prepared by Gaurav Agarwal [aka Gaurav]

VIII. PROTOCOL of POLICY ANALYTICS for CYBERSECURITY

It is difficult to overestimate the complexity of developing and implementing cybersecurity policies for cyber-physical system when the policy texts are distributed, in different formats, and appear somewhat ambiguous. While considerable advances have been made toward cohesion and coherence, directives remain rather conceptual and descriptive, and for the most part seemingly underspecified.

This situation continues to create a dilemma for policy analysis as well as implementation – especially for specifying with some confidence ***what*** is to be done***, why, when*** and ***where*** as well as ***how***.

We address the dilemma by developing a multimethod data-based approach to support policy a*nalytics* for metrics and *network* models to assist the user in practical ways. At this point we revisit select segments of materials reported earlier to provide a more coherent and integrated perspective.

8.1. Capturing Value of Policy

Again, full value and implementation of CSF for the *Proof-of-Concept* can be difficult to capture given:

a) the details and **complexity** of the conceptual smart grid NIST model,

b) the set of ***intervening tasks*** that are required,

c) the ***distributed nature*** of policy documents,

d) the **burden on users** to manage (a) to (c) and, therefore,

e) the need to create an **integrated on-demand** method for access to relevant information.

In short, given that directives for implementation of CSF (① in **Figure 3.5** are distributed across several individual documents, each hosting different guidelines, the user's task is to identify and make connections among them as needed. Moreover, modifications and updates by NIST on the content of key documents require users, in turn, to identify the updates and determine requirements for making changes to their initially integrated database.

Operationally, we create a suite of ***analytics-for-policy*** with operational methods to:

- Transend constraints of **policy-as text**,
- Transform text into **metrics**,
- Construct **models** of the system-state (the test case) based on system metrics,
- Connect models to **implementation** directives,
- Enable effective **linkages** among policy directives for cybersecurity, and
- **Target** specific "directive" to specific system **problem-point.**

Each item in the set usually consists of **several individual** but interconnected steps. So our approach is designed as ***end-to-end***, enabling user-determined focus on Whole-system or on select properties of the Whole.

We can begin with the ***system-as-is*** (i.e., the system model), and go through the process of implementing the ***Cybersecurity Framework*** with its diverse directives located in the different documents that provide implementation details. Alternatively, we can begin with the ***Cybersecurity Framework*** and its directives to identify and locate security requirements and then work toward application to the test-case system "As-Is".

Each "path" requires access to, and use of, interconnected directives, located in ***different policy document***s, and involves a set of specific tasks. The "devil is in the details".

CSF points to ***what*** has to be done and ***why.*** CSF also points to ***where*** the critical information is located in the distributed policy ecosystem. The user must work through the directives outlined by CSF for the system of interest; ***when*** is a **function** of the research design, as is ***how***.

8.2. Cybersecurity Framework (CSF)

Recall that the *Proof-of-Concept* of analytics for cybersecurity policy is the application of the NIST *Cybersecurity Framework* to the NIST conceptual model of smart grid system for electric power systems. All information pertaining to that case is derived from NIST's conceptual mode, itself based on expert panel conclusions.

8.2.1 Data Base

Here we refer once more to **Figure 3.5** presented earlier and the nine policy documents that serve as the raw data for different phases of the overall Project. Each policy document is ***autonomous***—i.e., on a standalone basis. Depending on the particular needs of the user—in terms of mission, industry, or other—drawing on diverse documents can be a necessity, not a choice.

Recall also that the number connected to each autonomous directive in **Figure 3.5 (**on core policy documents for "Text-to-Data**")** serves as an *identifier* for its use in the research design. Note, again, that some documents are (i) *sector independent* (ii) others pertain only to the test case, smart grid system, and (iii) still others are applicable more generally.

The research design requires the construction of operational linkages among data pertaining to system state and CSF policy features, noted earlier:

- ***System State,*** "As-Is," focusing on system actors and activities (labelled as nodes) and logical interfaces between,
- ***Security Objectives,*** as stated by NIST,
- ***Impact Level*** on nodes and logical interfaces,
- ***Properties of logical interface(s)*** between two nodes,
- ***Vulnerability Class*** of each node and logical interface, and
- ***Security Requirements*** for nodes and logical interfaces.

Earlier we presented the results for the computed **network** model of the NIST Conceptual Smart Grid as a cyber-physical system (see **Figure 4.6**). The model is derived from the metrics and measures embedded in the *Design Structure Matrix* of the NIST model, also shown earlier in **Figure 3.5**, referenced here to assist in situating the elements in **Figure 5.1** for illustrative purposes.

8.2.2 Security Requirements

At this point, the challenge is to Identify CSF security requirements and connect them to properties of the Proof-of- Concept model. Note the document identifiers for each step below:

a. **Implement** the connectivity protocol for application of CSF to the enterprise or system, using information in ①, ④ & ②;

b. **Determine** the technical, governance, compliance, and risk security requirements (from ④ & ②) for each logical interface, for H, M, L impact levels;

c. **Identify** the Cybersecurity Framework directives relevant to the *Proof-of-Concept* case using between documents ① and ④;

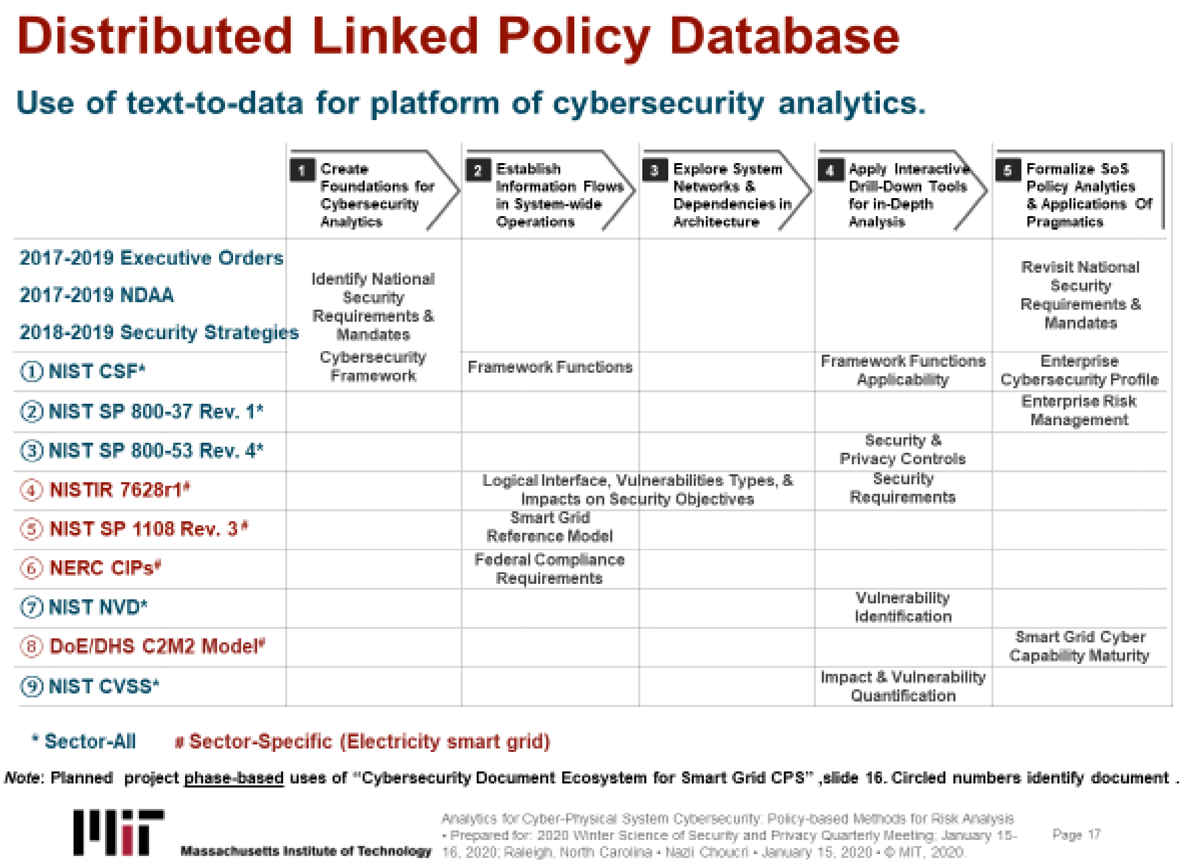
The expected value is to assist and enable the user, enterprise, or analyst, to implement CSF directives (and related requirements in ②, ⑦, and ⑨).

8.3. Distributed Policy Ecosystem

The nine policy texts for this Project, in **Figure 3.5,** are shown once more in **Figure 8.1** but ***distributed*** across different steps of the research design. Recall that **Figure 3.5** puts forth three sets of policy documents (each with directives and/or specified functions).

- Documents 1 – 3 pertain to CSF and supporting documents for its use.
- Documents 4 – 6 pertain to the *Proof-of-Concept*.
- Documents 7 – 9 have broad relevance and cover the entire sweep of cybersecurity initiatives.

The relevance of **Figure 8.1** at this point is not only that that it situates the key texts along the trajectory of the research design, but it also identifies the *specific* variables, associated with every *operational* function, at each step.



Distributed Linked Policy Database

Use of text-to-data for platform of cybersecurity analytics.

	1 Create Foundations for Cybersecurity Analytics	2 Establish Information Flows in System-wide Operations	3 Explore System Networks & Dependencies in Architecture	4 Apply Interactive Drill-Down Tools for in-Depth Analysis	5 Formalize SoS Policy Analytics & Applications Of Pragmatics
2017-2019 Executive Orders	Identify National Security Requirements & Mandates				Revisit National Security Requirements & Mandates
2017-2019 NDAA					
2018-2019 Security Strategies					
① NIST CSF*	Cybersecurity Framework	Framework Functions		Framework Functions Applicability	Enterprise Cybersecurity Profile
② NIST SP 800-37 Rev. 1*					Enterprise Risk Management
③ NIST SP 800-53 Rev. 4*				Security & Privacy Controls	
④ NISTIR 7628r1#		Logical Interface, Vulnerabilities Types, & Impacts on Security Objectives		Security Requirements	
⑤ NIST SP 1108 Rev. 3#		Smart Grid Reference Model			
⑥ NERC CIPs#		Federal Compliance Requirements			
⑦ NIST NVD*				Vulnerability Identification	
⑧ DoE/DHS C2M2 Model#					Smart Grid Cyber Capability Maturity
⑨ NIST CVSS*				Impact & Vulnerability Quantification	

* Sector-All # Sector-Specific (Electricity smart grid)

Note: Planned project phase-based uses of "Cybersecurity Document Ecosystem for Smart Grid CPS" ,slide 16. Circled numbers identify document .

Massachusetts Institute of Technology Analytics for Cyber-Physical System Cybersecurity: Policy-based Methods for Risk Analysis • Prepared for: 2020 Winter Science of Security and Privacy Quarterly Meeting; January 15-16, 2020; Raleigh, North Carolina • Nazli Choucri • January 15, 2020 • © MIT, 2020. Page 17

Figure 8.1: Sequence of Resort to Policy Texts

In a different vein, **Figure 8.2** shows a *highly stylized view* of ***sequence*** in the application of CSF It is presented here for largely contextual purposes.

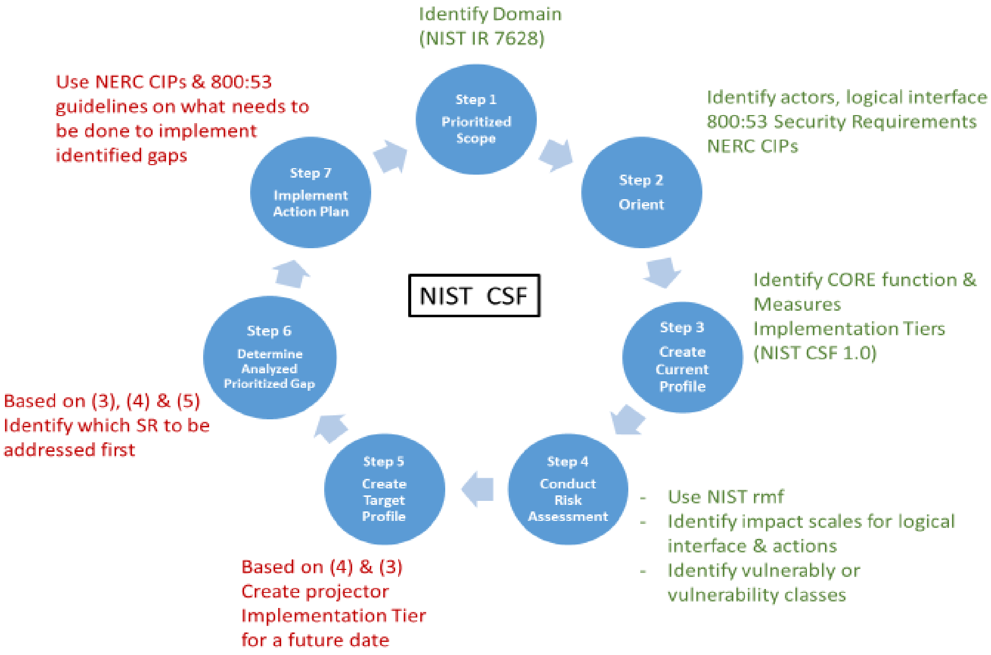


Figure 8.2: Stylized sequence of CSF Application

8.4. Operational Linkage System

By way of review, three important results require emphasis at this point:

One: The entire design process is completed and implemented it "top down", so to speak – i.e. starting from the *system-state* (in **Figure 4.1**).

Two: The operational information-linkages among documents that are essential for use, and/or implementation of CSF are completed.

Three: The initial pass through "bottom up" starts with the properties of the Cybersecurity Framework (step 6 in **Figure 8.1**) and then proceeds with application of the design back to the system-state (step 1).

Figure 8.3 focuses on a process tracing of system structure and linkages for policy. The Figure shows the pathways in the research design for implementation of CSF. Note the identifiers of individual ***policy*** documents, ***type*** of policy directive, and ***connection*** to system feature.

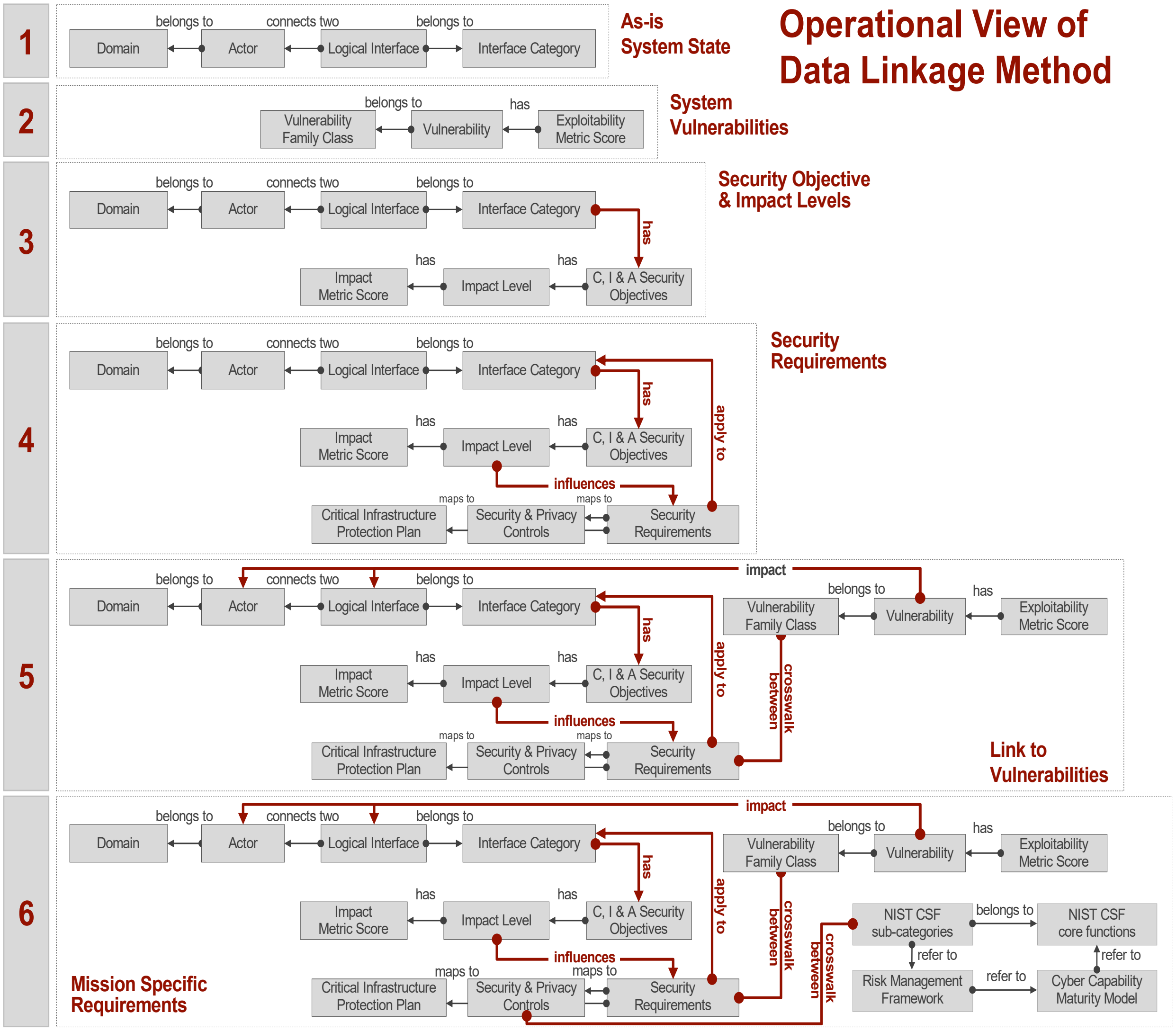


Figure 8.3: Process Tracing: **Operational view of data-linkage method**

Summarized by Gaurav Agarwal [aka Gaurav]

The **process tracing,** in **Figure 8.3**, illustrates the step-by-step sequence in the research design. The lineage of **Figure 8.3** can be traced to **Figure 3.1**, **Figure 4.1** and **Figure 5.1**. As such, it is evident **why** and **how** the process tracing in **Figure 8.3** highlights the operational tasks.

The next **Section** of this Compilation presents an added high-level perspective on the method and approach.

IX. REVIEW and AUDIT of POLICY ANALYTICS: END NOTE

This **Section** serves as a review of method and approach, and concludes with an “audit” of the research process.

9.1. Policy Problem

The overarching problem-area is three-fold:

One: Cybersecurity policies are developing faster than their implementation, but seemingly slower than emergent cyber threats.

- The lag is due in large part to barriers for user-access to guidelines. Operational directives often are located in different documents across the policy eco-system.
- Barriers of any type reduce the value of policies to protect systems (and users) from known vulnerabilities in their operations.

Two: Policies are usually articulated and presented in text form.

- Text means word after word, sentence after sentence etc. This form impedes precision and effective targeting to guidelines for “solution” of system “problem”.
- Capturing the value of policy depends on the precise representation of system-state as well as an accurate understanding of existing vulnerabilities and attendant impacts.

Three: Such situations require new operational solutions that can become “routine” and “normal”.

- Analytics for policy must target specific “directives”, or solutions at specific system problem-point.
- Effective targeting requires the application of an operational process at each step in a suite of analytics-for-policy.

The policy problem is not restricted to cybersecurity policies for cyber-physical systems. It is generic, relevant to all policy domains. Yet some elements in the solution strategies can be customized for specific contexts.

9.2. Operational Challenges

At the onset we recognized three “high level” challenges, the resolution of which is central to the research design.

First, to be rendered compliant with the CSF, system domains and the relevant properties must be identified clearly. This is essential in order to “map” the appropriate CSF directive on to the intended system property.

- *The challenge is to create a representations of system properties in metric terms to create a system model.*

Second, while for the most part the CSF directives are clearly stated and rich in details, as noted, the essential information is distributed across the entire cybersecurity policy ecosystem.

- *The challenge is to reduce the burden on users for locating specific directives of relevance***.**

Third, is to align CSF directives with the system model as accurately as possible.

- *The challenge is to address all system properties, at all levels of aggregation, and in all policy-relevant detail.*

In sum, the operation of effective analytics for policy depends on the precise representation of ***system-state*** as well as accurate understanding of the existing ***vulnerabilities***. At the onset, we recognized three “high level” challenges, the resolution of which is essential for the research design and the proof-of-concept.

9.3. Brief Highlights

The following *Highlights* focus on sequence of critical steps and expected results. Central to the entire enterprise is managing the *dependency structures* among directives and guidelines:

First, we begin with the ***Proof-of-Concept,*** the generic NIST conceptual model of **smart grid** for electric power systems ***as test-case,*** and:

- Create the ***system structure*** from the NIST model by its conversion to a Design Structure Matrix.

- Generate ***metrics*** of system properties from the DSM – and interconnections among properties – in order to generate a data-based representation.

- Transform the metrics-system into a ***network model*** of the test-case.

- Apply ***statistical methods*** *to* explore the significance of structural properties for the system model (i.e., actors, domains and interfaces).

Second, we focus on the ***Cybersecurity Framework*** for applications of the ***security*** objectives and ***requirements*** to the test case; and

- Identify the ***vulnerabilities*** of the system-As-Is in order to situate the security objectives and requirements.

- Determine the ***impacts of vulnerabilities*** following CVSS, aggregating vulnerabilities across system domains.

- Locate the security ***requirements*** for different security ***objectives***.

- Connect the security objectives and security requirements to the ***intended targets*** across system domains and properties.

<u>*Third*</u>, we identify and map the process tracing from the ***dependency structure*** among the critical documents in the relevant policy ecosystem, in **Figure 3.5** earlier, and differentiate between ***sector-specific*** directives and those of ***general application*** for cybersecurity policy.

We also signal in diagram form, **how** these documents bear on the Proof-of-Concept case, and identify each of the relevant the **specific** guidelines or variables **(Figure 8.3)**.

9.3.1. *Profile of the "Proof-of-Concept" Study*

Figure 9.1 below shown the key elements of the linkage process for vulnerabilities and security requirements

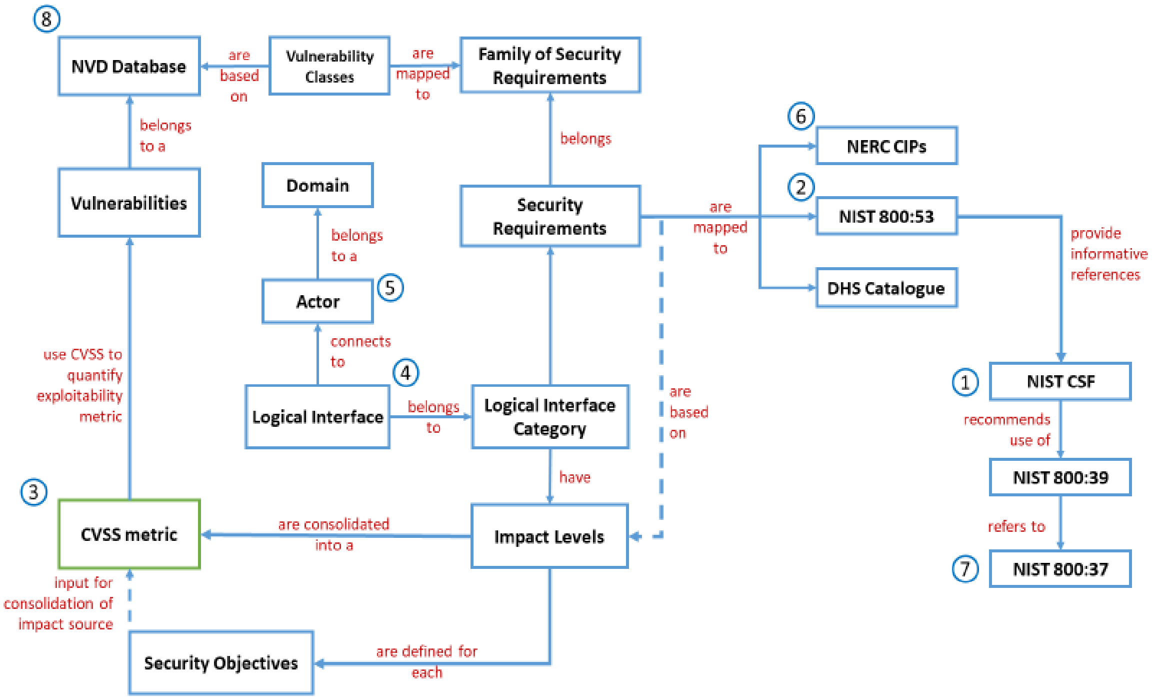


Figure 9.1: Aligning vulnerabilities and security requirements to the features of the Proof-of Concept system.
Summarized by Gaurav Agarwal [aka Gaurav]

The research design requires the construction of data sources and linkages for operational connections between (a) the system state and (b) the CSF policy features. By now, the list of steps noted frequently, and reported most recently in Section VIII, is very familiar.

9.3.2. *Principles of Practice*

Here we identify the three basic principles that create confidence in both process and product. These also serve as an "insurance policy" for effective use of time, resources, and skills.

One: ***Pre-test*** the method employed at every step, in order to *identify problems*, unanticipated barriers, or miscalculations or errors in the research design – and resolve these in advance.

Two: ***Post-test*** each step after completion, as relevant, *by reversing the process*.

Three: Demonstrate ***portability*,** by applying the core methods to issues, challenges, or cases beyond the focus, framework, or purpose of the *Proof-of-Concept*, to determine *stand-alone robustness.*

These are principles of choice – for purposes of assuring the quality of research. They are not set in formal obligations.

9.3.3. *Utility to the Enterprise*

Here we highlight some specific elements of utility to an enterprise.

The approach allows the enterprise to identify the particular categories and elements of the NIST Cybersecurity Framework **[1]** that are applicable to specific logical interface and actors (based on informative references between NIST CSF and security controls of NIST SP800:53 Rev.5) **[2]** to assist in prioritizing the enterprise use of its resources to:

a. Create domain/actor/logical interface specific cybersecurity micro-profiles, and

b. Aggregate individual micro-profiles into an enterprise-level macro-profile.

As such, the method facilities the assessment of cybersecurity vulnerabilities and requirements. The enterprise profile will be more quantitative as well as traceable because it can be linked to the current implementation state of selected security controls NIST SP800:Rev.5 **[2]**. The result is to:

a. Strengthen *current* implementation assessment of its cybersecurity profile.

b. Improve *future* implementation based on completion security controls that are applicable to its cybersecurity profile but not yet implemented.

Overall, this work enhances enterprise risk management because it allows for:

a. Use of standard-based sources and approach (such as NIST Risk Management Framework **[3]**, and Cyber Vulnerability Scoring System, CVSS, Ver.3.1 **[4], and** quantification of cybersecurity vulnerably

b. Determination of vulnerability impacts as well as their quantification.

All the above must be put to the test by the enterprise and to evaluate how best to proceed in an operational mode.

9.4. Audit of Analytics

The Audit-of-Analytics process consists of four key Imperatives introduced in this Project designed to enable the conduct of robust research for replicable results. These are defined as:

- **Coordinates of Design**
- **Policy Data for Cybersecurity**

- **Anchors for Analytics**
- **Challenges of the Unexpected**

We now address each Imperative:

9.4.1. *Coordinates of Design*

The coordinates of the Project research design consists of four *general* properties, plus one that carries some *particular* dilemmas. Each property is framed in comparative and binary idiom – that is (a) vs. (b). The purpose below is to address each of these coordinates.

- **Theory vs. Data**

The Project is framed almost entirely by data. In fact, “data” itself is a central, if not core, focus. At the same time, we find it necessary, even essential, to focus on theory in two distinct ways, namely, (a) theory for *construction* of data base and (b) theory for *analysis* of constructed data base.

- **Data vs. Metrics**

A range of challenges are involved in the process of identifying and collecting the relevant “raw” policy data. The challenge is to transform *text* data into organized *structure,* and to convert descriptors into for *metrics*, while at the same time: (a) retain the *integrity* of the source content, and (b) provide means for metric *verification* and validation.

- **Metrics vs. Methods**

Metrics are based on descriptors of organized structure derived from the “raw data”. Effective use of metrics begins with methods, followed by applications, replications, and validation, and the like – all to provide metrics accuracy. In this Project, we differentiate among methods by *context,* as follows:

(i) Method of the research design

(ii) Method for collection of data,

(iii) Method in generation of metrics, and

(iv) Method for analysis of metrics.

Each of (i) – (iv) is based on different criteria, depending on the system model, or the task at hand.

- **Methods vs. Models**

Methods refer to “tools” used to generate metrics (*per* the above). Metrics are basic and essential inputs for the construction and use of models.

Overall, this the *Proof-of-Concept* draws largely on three modes and models of method:

(i) Design structure matrix as *input* for network model;

(ii) "By hand" deep-description linkages of *content* linkages across distributed policy documents; and

(iii) Operational mapping policy *linkages* to properties of cyber-physical system.

Again, these can be used jointly or on a stand-alone basis – depending on user needs.

- **Process vs. Products**

The dilemma at this point, is that, for some purposes, process and products can be merged, but for other purposes these must remain separate. This distinction is not articulated nor is it anticipated in the research design, rather it evolves as a pragmatic matter.

9.4.2. *Policy-Data for Cyber-Physical Systems*

The second Audit Imperative focuses on the text form of the "raw data", and identifies specific operational properties that jointly define the research initiative.

- **Policy System vs. Cyber-Physical System**

Establishing connections between (a) policy directive, (b) cyber-physical system and (c) linkages between (a) and (b) is about data alignment.

Given that the challenge is to bring policy to bear on cyber-physical systems, we devote more attention to the properties of the cyber-physical system than to the logic of policy. We now recognize that we can give more attention to the *complexity of the polic*y domain and less to the *cyber-physical system* model.

- **Conceptual vs. Empirical**

A related feature of the second Imperative is the distinction between *conceptual* and *empirical* sources of data as reported in NIST 7628.

The research proceeds with the understanding that the conceptual model is created at the source and serves as "raw data" to represent the cyber-physical system. Thus, what is considered fundamental to system operations has *already* been defined by NIST 7628.

- **Empirical vs. Operational**

The value-added at this point is the successful construction of an *operational* model for the cyber-physical system, based on its properties framed in *empirical* terms.

- **Operation vs Implementation**

Implementation here refers to the value-added or net utility of modelling the system structure for the overall research design.

On the one hand, we construct data and metrics based on information in NIST 7628 conceptual representation of smart grid cyber-physical system. On the other hand, the full utility of such representation is contingent on applications of direct policy interventions to the system itself. We recognize this important difference.

- **Implementation vs Validation**

The implementation and validation of the research design carry a two-fold challenge:

(i) implementation of *cyber-physical system*, as well as validation, may be achieved by effective application of methods to other systems;

(ii) implementation for *policy and directives,* by contrast, as well as validation remain contingent on completion of the policy-cyber-physical system linkages.

9.4.3. *Anchors for Analytics*

The third Imperative of the audit system focuses on a six research *anchors,* termed as such since are also "stand alone" segments designed to support both *logic* and *process* for the overall Project.

- **System of Policies vs. System of Operations**

The most notable feature of the Project design is captured by the differences between (a) *policies* and directives (b) cyber-physical systems *operations*, and (c) the *linkage* mechanisms that relate (a) and (b) – to enable application, implementation, and validation.

- **Whole vs. Partial Design**

Here we define "Whole" as a *stand-alone system* of the research design, and "Partial" as an element *within* the "Whole". This distinction helps to identify and situate the functions of aggregation and disaggregation.

- **Parsing "Pieces"**

Connected, but not identical to the above, is *parsing,* defined to mirror the first Audit Imperative, namely coordinates of design. This element is pervasive throughout and greatly assists researchers to identify key features of coordinates as needed.

- **System vs. Network**

While these terms can commonly be seen as mirror images, identical, or overlapping, here we draw an important distinction. S*ystem* refers to the model representation of the cyber-physical entity of interest. *Network* refers to the transformation of the model into a network of actors and interfaces.

Recall that network representations of the cyber-physical system test case allow analysts to situate vulnerabilities, salience, and impacts.

- **Metrics vs. Statistics**

At the onset of this audit, we addressed the matter of *metrics*. Here we highlight our use of the common understanding of *statistics* as a *method* applied to metrics. The metrics signaled here represent the cyber-physical system; and the statistical analysis focuses on the distinguishing features of relevance to the test-case.

- **Static vs. Dynamic**

The *Proof-of-Concept* research design highlights policies and cyber-physical systems – both framed in *static* terms. At the same time, we recognize the importance of embedded *dynamics.* One of the cases we use for validation purposes -- reported in a companion Compilation -- demonstrates "feedback dynamics", a hidden feature embedded in system properties and apparent only with deep network analysis.

9.4.4. *Challenges of the Unexpected*

The last part of this ***audit-of-analytics*** identifies the issues or dilemmas not anticipated in the initial research design or in the first round of investigations. These include:

- **Policy vs. Policy Ecosystem**
- **Centralized vs. Distributed Directives**
- **Reporting vs. Results**
- **"The Devil is in the Details"**

It turned out that these issues are actually defining features of the very "reality" that we set out to examine. For this reason, they become added and persistent challenges:

- **Policy vs. Policy Ecosystem**

Our initial focus on NIST 7628 takes into account a wide range of system features included therein. As we dig deeper, it becomes clear that this document is foundational for the system "As-Is". The shift of focus from *policy* to *policy ecosystem* is due to the distributed nature of the policy directives.

Early on, we report the results of our work to build the entire policy ecosystem to capture directives and guidelines designed to connect cybersecurity policies to the *Proof-of-Concept* case. Then, as introduced in Section V, we come across a necessary "re-do" created by a new version of a key policy document.

- **Centralized vs. Distributed Directives**

By necessity, a corollary of the above is the need to deal with, and manage, a rather vexing feature of the policy ecosystem. Guidelines and directives are distributed across different documents. The user is responsible for identifying, linking, and integrating the new message.

This means that a massive data compilation must be undertaken in order to identify system features and policy targets. A similar must be done to connect *polic*y to *targe*t points in the cyber-physical system.

- **Reporting vs. Results**

Throughout the Project period, the practice is to report *accomplishments* for each quarter. In this process, the distinction between *reporting* accomplishments and highlighting *results* is often blurred or difficult to make.

This ambiguity is especially problematic when “accomplishments” are part of the process that leads to “results”. As noted earlier, the accomplishments reported at each stage are processes or products that are *necessary* to generate the next set of results.

- **“The Devil is in the Details”**

As a data-based and method-driven Project, we rapidly encounter the experience of “drowning in data” given the complexity of the policy ecosystem.

The sheer volume and micro-level details surrounding each individual guideline, for any one “actor” in the cyber-physical system, is daunting. In the absence of prior theoretical or conceptual logic, we resort to “sorting out” by “deep description”, as a prelude to the use of metrics.

9.5. Companion Compilation

This Compilation is focused on a “*Proof-of-Concept*” case. Concurrently a set of unrelated cases are undertaken as validation checks for the entire process off metricization – from initial text form all the way to the network model. These stand-alone cases, and the results, are reported in a companion Compilation venue.

The purpose of the companion Compilation is to guard against embedded bias during the phases of text-to-data, data-to-metrics, and metrics-to-model. By engaging in, and addressing, very diverse empirical cases, we generate insights and information that helps us consider the potential impact, if any, of case-*context* in the course of research-c*onduct*.

IX. END NOTE: REVIEW and AUDIT of POLICY ANALYTICS

References

1. National Institute of Standards and Technology (2020) Guidelines for Smart Grid Cybersecurity. (U.S. Department of Commerce, Washington, D.C.), Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, NISTIR 7628, Vol.1, REV.1. September 2014. https://doi.org/10.6028/NIST.IR.7628r1

2. National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53) (Rev. 5) (Sept. 2020 (includes updates as of Dec. 10, 2020)) https://doi.org/10.6028/NIST.SP.800-53r5

3. NIST Risk Management Framework (RMF). [Website] https://csrc.nist.gov/projects/risk-management/about-rmf

4. Common Vulnerability Scoring Systems version 3.1. FIRST.org https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

X. CONSOLIDATED REFERENCES

Section I – Introduction

1. Cyber Security Procurement Requirements Traceability for the Electric Sector, Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002003331, 2014. https://www.epri.com/#/pages/product/3002003255/

2. Security Posture using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002003332, 2014. https://www.epri.com/#/pages/product/3002003332/

3. Risk Management in Practice, Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002003333, 2014. https://www.epri.com/#/pages/product/3002003333/

4. Cyber Security Risk Management in Practice, Electric Power Research Institute, Palo Alto, CA, Tech. Rep. 3002004712, 2014. https://www.epri.com/#/pages/product/3002004712/

5. M. Harvey, D. Long and K. Reinhard, "Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security," 2014 Power and Energy Conference at Illinois (PECI), Champaign, IL, 2014, pp. 1-8. https://ieeexplore.ieee.org/document/6804566

6. D. Long, B. Drennan, and K. Reinhard, "NISTIR 7628 Visualization", Cyber Resilient Energy Delivery Consortium (cred-c.org). https://cred-c.org/sites/default/files/posters/19_SynchDataQ_Poster_CREDC%20IW%2017.pdf

7. B. Rogers and E. Gilbert, "Identifying architectural modularity in the smart grid: an application of design structure matrix methodology", Grid-Interop Forum, Phoenix AZ, 2011. https://sdm.mit.edu/news/news_articles/webinar_082012/rogers_082012.pdf

8. C. F. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," in IEEE Communications Magazine, vol. 51, no. 1, pp. 58-65, January 2013. https://ieeexplore.ieee.org/document/6400439

9. NIST, "Guidelines for Smart Grid Cybersecurity," NISTIR 7628, Revision 1. September 2014. https://doi.org/10.6028/NIST.IR.7628r1

10. Nicol, D., B. Sanders, J. Katz, B. Scherlis, T. Dumitraș, L. Williams, and M.P. Singh. 2015. Science of Security lablet: Progress on Hard Problems. p2. https://cps-vo.org/node/21590

Section II – Complexity of Cybersecurity Policy

1. United States, Executive Office of the President [Donald Trump]. “Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” *Federal Register*, 82 FR 22391, pp. 22391-22397. May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

2. Department of Defense, Summary; Donald J. Trump, National Cyber Strategy of the United States of America (Washington, DC: White House, September 2018), p.4. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
3. Department of Defense, Summary; Donald J. Trump, National Cyber Strategy of the United States of America (Washington, DC: White House, September 2018), p.5. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
4. Office of the Director of National Intelligence (2019) *National Intelligence Strategy of the United States of America*. January 23, 2019. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
5. H.R.5515 - 115th Congress (2017-2018) “John S. McCain National Defense Authorization Act for Fiscal Year 2019,” August 13, 2018. p.542. https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.
6. H.R.5515 - 115th Congress (2017-2018) “John S. McCain National Defense Authorization Act for Fiscal Year 2019,” August 13, 2018. p.502. https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

Section III – Proof-of-Concept: Database

1. National Institute of Standards and Technology (2020) *Guidelines for Smart Grid Cybersecurity*. (U.S. Department of Commerce, Washington, D.C.), Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, NISTIR 7628, Vol.1, REV.1. September 2014. https://doi.org/10.6028/NIST.IR.7628r1
2. Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework
3. National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53) (Rev. 4) (April, 2013) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
4. NIST Special Publication (SP) 800-82 Revision 1 Guide to Industrial Control Systems Security. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf
5. NIST 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations. (April, 2013) https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf
6. Open Web Application Security Project (OWASP) vulnerabilities. https://www.owasp.org
7. Common Weakness Enumeration (CWE) vulnerabilities. https://cwe.mitre.org
8. North American Electric Reliability Corporation (NERC), United States Mandatory Standards Subject to Enforcement: Critical Infrastructure Protection (CIP) Standards [Web page], http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20State

9. United States Code, 2012 Edition, Supplement 1, Title 44 - PUBLIC PRINTING AND DOCUMENTS. Added Pub. L. 107-347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947. p.148

10. United States Code, 2012 Edition, Supplement 1, Title 44 - PUBLIC PRINTING AND DOCUMENTS. Added Pub. L. 107-347, title III, §301(b)(1), Dec. 17, 2002, 116 Stat. 2947. p.147

11. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, February 2004. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

12. The National Infrastructure Protection Plan, Partnering to enhance protection and resiliency, Department of Homeland Security (DHS), 2009.

13. NRC Regulatory Guidance: Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment, version 1.0, NERC, June 14, 2002.

Section V – Security and Privacy

1. National Institute of Standard and Technology (NIST). (September 2020) NIST SP 800-53, Rev.5 Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Section VI – Research Fundamentals

1. National Institute of Standards, and Technology. Framework for improving critical infrastructure cybersecurity. 2014. https://www.nist.gov/cyberframework

2. M. Bastian, S. Heymann and M. Jacomy, "Gephi: an Open Source Software for Exploring Manipulating Networks", Association for the Advancement of Artificial Intelligence. 2009.

3. Jacomy M, Venturini T, Heymann S, Bastian M (2014) “ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software”. PLOS ONE 9(6): e98679. https://doi.org/10.1371/journal.pone.0098679

Section XI – Policy Analytics for Cybersecurity of Cyber-Physical Systems

1. National Institute of Standards and Technology (2020) Guidelines for Smart Grid Cybersecurity. (U.S. Department of Commerce, Washington, D.C.), Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, NISTIR 7628, Vol.1, REV.1. September 2014. https://doi.org/10.6028/NIST.IR.7628r1

2. National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems (NIST Special Publication 800-53) (Rev. 5) (Sept. 2020 (includes updates as of Dec. 10, 2020)) https://doi.org/10.6028/NIST.SP.800-53r5

3. NIST Risk Management Framework (RMF). [Website] https://csrc.nist.gov/projects/risk-management/about-rmf

4. Common Vulnerability Scoring Systems version 3.1. FIRST.org https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

Appendix I. PUBLICATIONS and WORKING PAPERS

PUBLISHED JOURNAL ARTICLES & CONFERENCE PROCEEDINGS

1. Choucri, N., & Agarwal, G. (2022a). Analytics for cybersecurity policy of cyber-physical systems. *Proceedings of the 2022IEEE International Symposium on Technologies for Homeland Security (HST)*, forthcoming, *pre-print* https://hdl.handle.net/1721.1/146916
2. Dahan, M., Amin, S., Jaillet, P. (2021) Probability distributions on partially ordered sets and network interdiction games. *Mathematics of Operations Research 47*(1), 458–484.
3. Choucri, N., & Agarwal, G. (2021). Complexity of international law for cyber operations. *Proceedings of the 2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, 1–7. https://dspace.mit.edu/handle/1721.1/141741
4. Klemas, T., Lively, R., Atkins, S., & Choucri, N. (2021). Accelerating cyber acquisitions: Introducing a time-driven approach to manage risks with less delay. *The ITEA Journal of Test and Evaluation, 42*, 194–202. https://dspace.mit.edu/handle/1721.1/141745
5. Choucri, N., & Agarwal, G. (2019). Securing the long-chain of cyber-physical global communication infrastructure. *Proceedings of the 2019 IEEE International Symposium on Technologies for* Homeland *Security (HST)*, 1–7. https://dspace.mit.edu/handle/1721.1/141740
6. Klemas, T., Lively, R. & Choucri, N. (2018). Cyber acquisition: Policy changes to drive innovation in response to accelerating threats in cyberspace. *Proceedings of the 2018 International Conference on Cyber Conflict (CYCON U.S.)*, 103–120. https://dspace.mit.edu/handle/1721.1/141746
7. Choucri, N., & Agarwal, G. (2017). Analytics for smart grid cybersecurity. *Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, 1–3. https://dspace.mit.edu/handle/1721.1/141738

PROJECT WORKING PAPERS

1. Choucri, N., & Agarwal, G. (2022b). *Complexity of international law for cyber operations* (Research Paper No. 2022-10). MIT Political Science Department. https://dspace.mit.edu/handle/1721.1/141742
2. Choucri, N., Fairman, L., & Agarwal, G. (2022). CyberIR@MIT: Knowledge for science, policy, practice (Working Paper No. 2022-09). MIT Political Science Department. https://dspace.mit.edu/handle/1721.1/141744
3. Choucri, N. (2021a). *New Hard Problems in Science of Security* (prepared for Symposium in the Science of Security (HotSoS). MIT Political Science Department.
4. Moulton, A., Madnick, S. E., & Choucri, N. (2020). *Cyberspace operations functional capability reference architecture from document text* (Working Paper CISL# 2020-24). MIT Sloan School of Management. https://dspace.mit.edu/handle/1721.1/144159
5. Choucri, N., Agarwal, G., & Koutsoukos, X. (2018a). *Policy-governed secure collaboration: Toward analytics for cybersecurity of cyber-physical systems* (Working Paper). MIT Political Science Department. https://dspace.mit.edu/handle/1721.1/141743

RELATED PUBLICATIONS DURING PROJECT PERIOD

Book

1. Choucri, N., & Clark, D. D. (2019). *International relations in the cyber age: The co-evolution dilemma*. MIT Press. https://mitpress.mit.edu/9780262038911/

Book Chapter

2. Choucri, N. (2021b). Framework for an artificial intelligence international accord. In N. A. Tuan (Ed.), *Remaking the world: Toward an age of global enlightenment* (pp.27–44). Boston Global Forum, United Nations Academic Impact. https://dspace.mit.edu/handle/1721.1/141737

Working Papers

3. Choucri, N. (2022a). *Ethics in Artificial Intelligence: Toward Foundations for Global Policy* (Working Paper). MIT Political Science Department. https://hdl.handle.net/1721.1/146915
4. Dukakis, M., Vike-Freiberga, V., Cerf, V., Choucri, N., Lagumdzija, Z., Nguyen, T. A., Patterson, T., Pentland, A., Rotenberg, M., & Silbersweig, D. (2020). *Social contract for the AI age.* Artificial Intelligence World Society (AIWS), & Michael Dukakis Institute for Leadership and Innovation. https://dspace.mit.edu/handle/1721.1/144065
5. Dukakis, M., Nguyen, T. A., Choucri, N., & Patterson, T. (2018). *The concept of AI-government: Core concepts for the design of AI-government* (Concept Paper). Boston Global Forum, & Michael Dukakis Institute for Leadership and Innovation. https://dspace.mit.edu/handle/1721.1/144064
6. Dukakis, M., Choucri, N., Cytryn, A., Jones, A., Nguyen, T. A., Patterson, T., Reveron, D., & Silbersweig, D. (2018). The AIWS 7-layer model to build next generation democracy. *BGF-G7 Summit 2018*. The Boston Global Forum, & Michael Dukakis Institute for Leadership and Innovation. https://dspace.mit.edu/handle/1721.1/144063

WEBPAGES on SCIENCE OF SECURITY WEBSITE

Following content related to *lablet spotlight*, and *news* were submitted to Science of Security Virtual Organization website.

1. Choucri, N. (2023b, January 19). *Decoding EU-GDPR* [News]. https://cps-vo.org/node/92718
2. Choucri, N. (2023c, January 3). *Framework for AI global accord* [News]. https://cps-vo.org/node/91797
3. Choucri, N. (2023d, January 3). *Cyberspace & sustainability* [News]. https://cps-vo.org/node/91796
4. Choucri, N. (2022b, September 30). *International relations in the cyber age: The co-evolution dilemma* [Book Announcement]. https://cps-vo.org/node/91415
5. Choucri, N. (2022c, April 27). *Analytics for cyber-physical systems cybersecurity* [Spotlight on Lablet Research #29]. https://cps-vo.org/node/83878

6. Choucri, N. (2020c, January 03). *Analytics for cyber-physical systems cybersecurity* [Spotlight on Lablet Research #1]. https://cps-vo.org/node/64483

Appendix II. PROJECT REPORTS

SoS QUARTERLY LABLET MEETINGS PRESENTATIONS

Project progress -- presented at the following SoS Quarterly Lablet meetings : follows:

1. Choucri, N. (2021c, July 13–14). *Analytics of cybersecurity policy: Value for artificial intelligence?* [Conference session]. Summer 2021 Quarterly Science of Security Lablet Meeting, online. https://cps-vo.org/LabletQTRLY/2021/CMU-register
2. Choucri, N. (2021d, April 12–15). *Special session on Science of Security hard problems: Rethinking security measures* [Conference session]. 2021 Symposium in the Science of Security (HotSoS), online. https://cps-vo.org/node/75159
3. Choucri, N. (2020c, January 15–16). *Application of policy-based methods for risk analysis* [Conference session]. Winter 2020 Quarterly Science of Security and Privacy Lablet Meeting, Raleigh, North Carolina. https://cps-vo.org/LabletQTRLY/2020/NCSU
4. Choucri, N. (2019, July 9–10). *Analytics for cybersecurity of cyber-physical systems—Overview and Year 1 report* [Conference session]. Summer 2019 Quarterly Science of Security and Privacy Lablet Meeting, Lawrence, Kansas, United States. https://cps-vo.org/LabletQTRLY/2019/KU; https://cps-vo.org/node/61617
5. Choucri, N. (2018b, July 31 and August 1). *Panel on transition: Panel with representatives from each lablet on ideas to make transition successful*. Summer 2018 Quarterly Science of Security and Privacy Meeting, Urbana, Illinois, United States. https://cps-vo.org/LabletQTRLY/2018/UIUC
6. Choucri, N. (2018c, March 13–14). *Project kick-off* [Conference session]. Science of Security Lablet Kickoff and Quarterly Meeting, College Park, MD, United States. https://cps-vo.org/SoSLabletQtrlyMeeting_2018

SoS QUARTERLY LABLET MEETINGS PARTICIPATION

MIT PI participated in the following Quarterly Lablet meetings:

1. *2021 Winter Quarterly Science of Security and Privacy Lablet Meeting,* January 12–13, 2021, online. https://cps-vo.org/LabletQTRLY/2021/VU
2. *2019 Fall Quarterly Science of Security and Privacy Lablet Meeting*, Chicago, Illinois, November 5–6, 2019; https://cps-vo.org/SoSLmtg/UIUC/2019
3. *6th Annual Hot Topics in the Science of Security (HoTSoS) Symposium*, Nashville, Tennessee, April 1–3, 2019. (as member of organizing committee) https://cps-vo.org/node/60225
4. *2019 Winter Quarterly Science of Security and Privacy Lablet Meeting*, Berkely, CA, January 10–11, 2019. https://cps-vo.org/LabletQTRLY/2019/icsi
5. *2018 Fall Quarterly Science of Security and Privacy Lablet Meeting,* Carnegie Mellon University (CMU), October 29–30, 2018. https://cps-vo.org/node/55841

OUTREACH: SELECT EVENTS by INVITATION

Works completed under this project were presented at the following meetings & conferences:

1. Choucri, N. (2023a, January 19). *New Realities—New Challenges* [Online Talk]. MIT Industrial Liaison Program Event. https://ilp.mit.edu/Geopolitics
2. Choucri, N. (2020a, December 2–3). *The dynamics of cyberpolitics* [Conference session]. CyberSecure 2020, online. https://emtech.technologyreview.com/cyber-secure-2020/
3. Choucri, N. (2020b, November 12–13). *The Quad Group, AIWS social contract and solutions for world peace & security* [Conference session]. Riga Conference 2020, online. https://archive2.rigaconference.lv/2020/index.html
4. Choucri, N., & Agarwal, G. (2020, July 10). *Analytics for Cybersecurity Policies of Cyber-Physical Systems: Policy-based Methods for Risk Analysis* [Conference presentation]. CAMS Research Group Lunch Meeting, MIT Sloan Management School. Meeting link https://mit.zoom.us/j/476825760
5. Choucri, N. (2018a, October 19–20). *Bytes and bullets: The future of cyber warfare* [Panel session]. New World Powers: Global Security Forum, Hartford, CT, United States. https://ctwac.org/event/global-security-forum-new-world-powers/

POSTERS

Prepared for research meetings at MIT:

1. Choucri, N., Madnick S., & Agarwal G. (2018b, July 16). *Analytics for Cybersecurity of Cyber-Physical Systems* [Conference & Poster session]. Cybersecurity at MIT Sloan Annual Conference: Answering the Question "How Secure Are We"? MIT Sloan School of Management, Cambridge, MA. https://cps-vo.org/sites/default/files/u15348/20180327_Analytics_for_Cybersecurity_of_CPS_Poster_for_IC3_April_Meeting.pdf
2. Choucri, N., & Agarwal G. (2022c). *Analytics for Cybersecurity of Smart Grid: Identifying Risk and Assessing Vulnerabilities* [Poster]. MIT Political Science, Cambridge, MA. https://cps-vo.org/sites/default/files/u15348/20220901a_Project_Summary_Poster.pdf
3. Choucri, N., & Agarwal G. (2022d). *Managing Risk: Capturing Full-Value of Cybersecurity Guidelines* [Poster]. MIT Political Science, Cambridge, MA. https://cps-vo.org/sites/default/files/u15348/20220901b_Managing_Risk_Poster.pdf
4. Choucri, N., & Agarwal G. (2022e). *Analytics for Enterprise Cybersecurity: Management of Smart Grid Cyber Risks & Vulnerabilities* [Poster]. MIT Political Science, Cambridge, MA. https://cps-vo.org/sites/default/files/u15348/20220901c_Analytics_for_Enterprise_Cybersecurity-Smart_Grid_Poster.pdf
5. Choucri, N., & Agarwal G. (2022f). *Analytics for Enterprise Cybersecurity Application Example Summary* [Poster]. MIT Political Science, Cambridge, MA. https://cps-vo.org/sites/default/files/u15348/20220901d_Analytics_for_Enterprise_Cybersecurity-CaseStudyPoster.pdf