Generation of Compliance Graphs Across Industries for Providing an Analysis Testbed

NOAH L. SCHRICK, Information Technology Laboratory, U.S. Army Corps of Engineers, Engineer Research and Development Center, USA

PETER J. HAWRYLAK, Tandy School of Computer Science, College of Engineering and Computer Science, The University of Tulsa, USA

Compliance graphs provide the ability to analyze an environment in terms of its standing to a regulation, mandate, or standard. These graphs are directed acyclic graphs, and share commonalities with attack graphs. Though generator tools and example graph sets are available for attack graphs, the novelty of compliance graphs presents its own set of challenges with a lack of publicly available data that has been processed and formatted in order to generate example graphs. In order to develop analysis techniques for compliance graphs, thorough examination and testing processes should be conducted, particularly on known, available data sets in the form of compliance graphs or compliance graph input files. This work presents the generation of compliance graphs and releases their affiliated data for use in furthering the analysis process of this research area.

CCS Concepts: • **Social and professional topics** → **Computing / technology policy**; • **Computer systems organization** → *Dependable and fault-tolerant systems and networks*; • **Computing methodologies** → **Model development and analysis**; • **Information systems**; • **Software and its engineering** → *Software organization and properties*;

Additional Key Words and Phrases: Compliance Graph, Attack Graph, Automotive Industry, Healthcare Industry, HIPAA, Oil and Gas Industry, OSHA 1910H

ACM Reference Format:

Noah L. Schrick and Peter J. Hawrylak. 2024. Generation of Compliance Graphs Across Industries for Providing an Analysis Testbed. 1, 1 (October 2024), 14 pages. https://doi.org/XXXXXXX.XXXXXXX

Authors' Contact Information: Noah L. Schrick, Noah.L.Schrick@erdc.dren.mil, Information Technology Laboratory, U.S. Army Corps of Engineers, Engineer Research and Development Center, Vicksburg, Mississippi, USA; Peter J. Hawrylak, peter-hawrylak@utulsa.edu, Tandy School of Computer Science, College of Engineering and Computer Science, The University of Tulsa, Tulsa, Oklahoma, USA.

ACM XXXX-XXXX/2024/10-ART
https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

Attack graphs are a common tool used to address and examine a system or set of systems under a cybersecurity lens [1]. These graphs are directed acyclic graphs (DAGs) that present the paths from a state of information for an environment to any potential state of vulnerability. Compliance graphs [2] aim to shift the focus of attack graphs to focus on the standings of environments to any local, private, or federal regulations. Each node in a compliance graph can be embedded with information regarding maintenance schedules for industrial equipment, insurance policy terms, physical component characteristics, or any other descriptor for an asset as it relates to an environment's standing toward compliance. Each edge in the compliance graph defines the transition that leads to a deviation in a previous node's information. These changes could include a repair or replacement of a component, the addition or removal of an asset, or changes to policies. Work and investigations have already been conducted to present the semantic and generator tool changes required to generate these graphs [3]. Though the generation of compliance graphs has been the primary focus of the research topic, there is an increasing need of analysis work to address the challenges of maintaining compliance. Governance, Risk, and Compliance (GRC) Officers assist groups or organizations with preventing or mitigating incurred costs as a result of a violation of a mandate. With the wide array of mandates that organizations may need to follow regarding health or personally identifiable information (PII), specific industry standards such as FinCEN [4], FDA QSR [5], NERC-CIP [6], internal standards, or equipment maintenance schedules to avoid voiding a warranty, it becomes increasingly difficult for GRC Officers to manage and track all mandate statuses. In addition, organizations rapidly and frequently bring changes into environments with new software, new equipment, new products, new contracts, or new processes. Each of these changes propagates additional change, all of which may affect the standing in regard to a compliance or regulation mandate. Rather than manual compliance checks, compliance graphs can be automatically generated, and analysis can be conducted on the resulting graph to aid in decision-making and visualization.

To determine the adaptivity and soundness of compliance graph analysis work, example networks across multiple, disconnected sectors are generated in this work for future analysis use. These sectors maintain their own different set of local, private, and federal regulations that must be adhered to in order to avoid penalties. For the generated examples, each additionally possesses unique characteristics and properties that allow for the examination of the depth and range of any compliance graph analysis techniques, especially under the consideration of edge cases or unexpected behaviors. To fully examine the accuracy and level of analysis output detail, this work strove to generate example cases that were accurately sourced, described fully, scalable, and of high fidelity. This work presents and describes the example networks that can be used and referenced for future compliance graph analysis works. Section 2 describes the Automobile Maintenance application that falls under the automotive industry. Section 3 describes a small network of healthcare clinics striving to maintain HIPAA [7] compliance through the lens of the healthcare industry. Section 4 describes an engineering firm as they attempt to maintain compliance with OSHA Standard 1910 Subpart H (Hazardous Materials) [8] within the oil and gas industry of the energy sector. Each of these example networks has been made publicly available, and their data files can be found at [9].

For each example network in the subsequent Sections, their properties are described. These properties are defined below. Each compliance graph was generated using a modified version of RAGE [10].

- Nodes: The number of states in the network that contain embedded information.
- Edges: The number of edges in the network that caused a change or deviation from a prior state.
- Exploits: The number of events, mandates, regulations, or checks that are investigated.
- Assets: The number of entities in the network or environment. Examples include devices, vessels, people, policies, etc.
- Qualities: The total number of descriptors for all assets. Examples include versions, make or model, material, policy limits, etc.
- Average Degree: The average number of new nodes that a node directs to.

2 Automotive

The automotive industry is a substantial sector in the United States, and is one of the largest automotive markets globally [11]. This industry invests $7.5 billion in innovative R&D, supports over 500,000 direct jobs in the US alone, has a Foreign Direct Investment of over $115 billion, and expands the US exports by over $56 billion [11], [12], [13], [14], [15]. This work includes a compliance graph within this sector as a means to showcase its application and utility for analyzing cost-savings and methodologies for following compliance mandates. Specifically, this work examines the Automotive Repair and Maintenance Service subsector of this industry. This subsector is globally applicable, and has a wide range of focal points and scale that include personal passenger vehicle maintenance and commercial vehicle servicing. This market has an estimated CAGR (Compounded Annual Growth Rate) of 10.2%, and passenger car maintenance holds a market share of 35% [16]. Due to the size of this market share, its applicability, its ease-of-understanding in compliance graph format, and its ability to scale to larger, more complex challenges in the automotive industry, this work generates and analyzes an automobile maintenance compliance graph. This Section discusses the generation process, graph properties, unique features, and incurred challenges with this example application.

2.1 Network Properties, Data, and Violation Specifications

The automobile maintenance example is centered around the maintenance of a single, 2006 Toyota Corolla over the span of 6 years. For this example, the compliance requirements follow the provided warranty and maintenance specifications as provided by the vehicle manufacturer. This document is accessible through the manufacturer's website [17]. The maintenance schedule provides the recommended maintenance routine based on either mileage or time since last maintenance, depending on which condition is met sooner. Following the recommended maintenance schedule is imperative to comply with any vendor or purchaser warranty, as well as to ensure proper operating conditions of the vehicle. Compliance graph generator input files were created following the maintenance document, and the properties for the generated automotive maintenance compliance graph are listed below.

- Number of Nodes: 66,945
- Number of Edges: 468,221
- Number of Exploits: 28
- Number of Qualities: 93
- Number of Assets: 1
- Average Degree: 6.994

Properties and assumptions of the Toyota Corolla are listed below.

- The vehicle is brand new, with 0 miles.
- It has a gas engine.
- It is an automatic.
- It includes a daytime running light system.
- The owner will perform minimal maintenance every 6 months or 6000 miles:
  - Oil and fuel filter change.
  - AC filter replacement.
  - Maintain proper tire pressure.
- The owner will take the vehicle to a mechanic shop every 1 year and 6 months for the following inspections and repairs:
  - Drive Belts
  - Battery
  - Spark Plugs
  - Brake Pedals
  - Brake Pads and Discs
  - Tires (Pressure, Alignment, Rotation)
  - Lights, Horn, Wipers, Windshield Washers
  - Refrigerant and Coolant
- Additional components modeled in this compliance graph include:
  - Fuel tank lines
  - Steering wheel, linkage, and gear box
  - Brake pipes and hoses
  - Drive shaft boots
  - Suspension ball joints
  - Front and rear suspensions
  - Fuel tank cap, lines, connections, and fuel vapor control valve

For this example, there is a single asset used to represent the 2006 Toyota Corolla. All parts, maintenances, timelines, properties, or any other features or components were considered to be a “quality" of the asset. By reducing the example graph to center around a single asset, state space explosion is able to be mitigated by preventing the deviation and permutation exploration of assets. Various exploit locks and flags were also implemented to prevent diverting, duplicated branches of simultaneous exploit triggers. This was implemented through the use of precondition guarding, and was necessary since exploits could be fired through either time or mileage, but should only be fired once. Additionally, the problem space was able to be reduced through the use of combined events. Rather than having exploits or events contain single quality changes, events could be grouped to update multiple qualities simultaneously. This was implemented through maintenance events, which acted as the single point of action for all inspections, repairs, maintenances, or any other

event that would service the vehicle and return it to a state of compliance. To further prevent divergence, all pre-defined events were also described using locks and flags, so the event (e.g. a traffic citation for a broken brake light) would happen a single time at a specific point in the generation.

The data sourcing for the violation specifications and prior-knowledge network consisted of maintenance and repair estimates at large, as well as for individual components or malfunctions. This also included mileages per year, by month, and various other personal automobile transportation statistics. Sourcing was collected from government entities like the Department of Energy [18], Department of Transportation [19], and Federal Highway Administration [20], aggregated car performance, reliability, and safety reports from Consumer Reports [21], and insurance companies like AAA [22], Farmers [23], and external reports [24]. At the time of this release, the prior-knowledge network is undergoing additional formatting and feature work before its release. The prior-knowledge networks are intended to be added to the released dataset, and the initial work is described in this publication. The prior-knowledge network contained additional detail about each exploit in the network. For each exploit, the cost of occurrence was described. These costs were expressed as one-time monetary costs, recurring monetary costs and their rate of charge, and one-time time-commitment costs, recurring time-commitment costs and their rate of charge. For each exploit, possible mitigation schemes were described. Each exploit could have zero or many mitigation options. Each mitigation option described one-time monetary costs, recurring monetary costs and their rate of charge, and one-time time-commitment costs, recurring time-commitment costs and their rate of charge for preventing the exploit. For this example, most exploits had at least one mitigation that was represented as a maintenance or service event.

2.2 Objectives and Goals of the Network

The primary objective of this example is to highlight the usefulness of the analysis methods for small, individual scale problems. Though the analysis methods are intended to work at a large scale, showcasing the utility of the approaches at a daily, understandable, personal level can lead to a greater adoption. In addition, this example network has unique properties not seen in the other example networks. This network is isolated to a single asset to highlight how the analysis methods can function even when centered on only one object of interest. Budgetary constraints are allocated at a monthly rate, rather than through lump sums. Many individuals may be able to allocate a limited amount of their monthly income to repairs and maintenance, but may have a more difficult time paying for unexpected costs and repairs all at once. This example includes a large number of qualities in proportion to the number of assets, and bolsters how effective the analysis techniques are when given more information. This example showcases how repeated, consistent, small-scale investments in repair and maintenance pay off significantly over the lifespan of a vehicle in terms of avoided malfunctions, damages, or fines.

3 Healthcare

The healthcare industry is another significant sector in the United States, and accounts for 17.3% of the GDP [25–28]. National Health Expenditures (NHE) have grown to over $4.5 trillion [25–29], Medicare and Medicaid spending have grown to over $944 billion and over $805 billion, respectively [25, 28, 30], R&D spending has grown to over $114 billion spread across biotechnology,

nanotechnology, and software [31] (with $83 billion in the pharmaceutical industry alone [32]), and there are over 6,100 [33] hospitals, 10,200 urgent care clinics [34], and 938,000 active physicians [35]. This work includes a compliance graph within this sector as a means to showcase its application and utility for analyzing cost-savings and methodologies for following compliance mandates. This work examines compliance of the Health Insurance Portability and Accountability Act (HIPAA) [7]. This is a broadly applicable federal act that mandates proper handling for the containment and dissemination of all healthcare information. HIPAA complaints have now exceeded 350,000, with 2,074 complaints being referred to the U.S. Department of Justice [36]. A total dollar amount exceeding $142 million has been collected as a result of noncompliance [37]. The Office for Civil Rights of the U.S. Department of Health and Human Services have reported the following as the most common occurrences of noncompliance complaints [37]:

- "Impermissible uses and disclosures of protected health information."
- "Lack of safeguards of protected health information."
- "Lack of patient access to their protected health information."
- "Lack of administrative safeguards of electronic protected health information."
- "Use or disclosure of more than the minimum necessary protected health information."

Due to the applicability of HIPAA to all healthcare related activities and processing, the quantity of noncompliance complaints, and the total monetary collection as a result of noncompliance, this work generates and analyzes a HIPAA compliance graph. This Section discusses the generation process, graph properties, unique features, and incurred challenges with this example application.

3.1 Network Properties, Data, and Violation Specifications

The HIPAA example is centered around a network of urgent care clinics and their compliance to HIPAA over the span of one year. For this example, the compliance requirements follow the provided guidelines as set by HIPAA. Since this is a federal regulation, specific guidelines and mandates are publicly accessible through the U.S. Department of Health and Human Services, as well as with summaries through the Center for Disease Control. HIPAA necessitates a range of requirements be met to ensure compliance, which include document control, training, reporting options, officers, physical and digital access control, and mandatory assessments. Compliance graph generator input files were created following the HIPAA guidelines, and the properties for the generated HIPAA compliance graph are listed below.

- Number of Nodes: 62,217
- Number of Edges: 400,917
- Number of Exploits: 27
- Number of Qualities: 62
- Number of Assets: 5
- Average Degree: 6.444

Properties and assumptions of the urgent care clinics are listed below.

- Each clinic has five employees.
- The organization has an in-house IT staff (that is **not** modeled).

- Each clinic will submit a HIPAA attestation letter.
- HIPAA attestation letters are not sent simultaneously.
- Each employee has a different renewal date for their trainings.
- Employee trainings and requirements enforced by the organization include the following:
  - HIPAA training.
  - Mobile and/or portable device regulation agreements.
  - Hardware inventories.
  - Security awareness.
- There are three total, distinct HIPAA officers:
  - HIPAA Compliance Officer
  - HIPAA Privacy Officer
  - HIPAA Security Officer
- Audits and assessments include:
  - Security risk assessment.
  - Privacy standing audit.
  - HIPAA audit.
  - Security standing audit.
  - Physical audit.
  - Device and asset audit.
- Additional components modeled in this compliance graph include:
  - An encrypted database.
  - Reporting processes.
  - A “company" asset that is independent of the employee and database assets.
  - Certificate expirations.

For this example, multiple assets are implemented to capture and model their relationships individually, as well as to other assets. These assets include employee assets, a database asset, and a company asset which is used to model the organization overall. Each asset had its own set of qualities, and their own quality for measuring the progression of time. In order to prevent unnecessary state space exploration on unfeasible states caused by a deviation in time progression, a synchronous firing feature [38] in the generator tool was used. Various exploit locks and flags were also implemented to prevent diverting, duplicated branches of simultaneous exploit triggers. This was implemented through the use of precondition guarding, and was necessary since exploits could be fired through multiple conditions, but should only be fired once. Additionally, the problem space was able to be reduced through the use of combined events. Rather than having exploits or events contain single quality changes, events could be grouped to update multiple qualities simultaneously. This was implemented through audit, assessment, or time-based events, which acted as a single point of action for all assessments, audits, services, or any other event that would correct any violation and return the organization to a state of compliance. To further prevent divergence, all pre-defined events were also described using locks and flags, so the event (e.g. an addition to or the removal of the number of employees) would happen a single time at a specific point in the generation.

The data sourcing for the violation specifications and prior-knowledge network consisted of imposed civil monetary penalties for noncompliance, time closures for noncompliance, and implementation or mitigation costs to prevent a compliance violation. At the time of this release, the prior-knowledge network is undergoing additional formatting and feature work before its

release. The prior-knowledge networks are intended to be added to the released dataset, and the initial work is described in this publication. The penalty structure as set by the Office for Civil Rights (OCR) consists of four tiers. Tier 1 is defined as a lack of knowledge of the violation, Tier 2 is for having reasonable cause for possessing knowledge of the violation, Tier 3 is for willful neglect, and Tier 4 is for willful neglect and a lack of correction within 30 days. Each tier has an associated minimum and maximum, with annual caps. These violations are stipulated by the Office of Management and Budget (OMB). In addition, the U.S. Department of Health and Human Services publishes a yearly summary of all OCR HIPAA settlements and judgments [39]. Reports to Congress [40], audits [41], and case examples [42] are also published. The prior-knowledge network was constructed around all publicly available sources, and contained additional detail about each exploit in the network. For each exploit, the cost of occurrence was described. These costs were expressed as one-time monetary costs, recurring monetary costs and their rate of charge, and one-time time-commitment costs, recurring time-commitment costs and their rate of charge. For each exploit, possible mitigation schemes were described. Each exploit could have zero or many mitigation options. Each mitigation option described one-time monetary costs, recurring monetary costs and their rate of charge, and one-time time-commitment costs, recurring time-commitment costs and their rate of charge for preventing the exploit. For this example, most exploits had two mitigations. This will be described further in Section 3.2.

3.2 Objectives and Goals of the Network

The primary objective of this example is to highlight the usefulness of the analysis methods for broadly applicable regulations. Though the input for this specific example was a network of urgent care clinics, the methods, procedure, and output would be largely similar to an input of a pharmacy, hospital, or biotechnology company. In addition, this example network has unique properties not seen in the other example networks. This network includes the addition and removal of employees, and attempts to mimic the behaviors of individuals. Though no claims of human behavior modeling is claimed, this work statically made events that were executed during the generation process as a way to represent human error (such as failing to complete a mandatory training). For the analysis of this work, this example showcases how a company could invest more time, rather than money, to maintain compliance. Most mitigatable exploits include at least two mitigations: one for contracting a correction, and one for utilizing the in-house staff. The contracting option requires minimal time cost, but has a greater monetary cost. The in-house implementation requires minimal monetary cost, but a greater time cost. This allows for the analysis to offer more robust correction schemes that can utilize both the monetary and time budgets to minimize and correct compliance violations.

4 Oil and Gas

The oil and gas industry contributes roughly 8% of the U.S. GDP, totaling to nearly $1.7 trillion [43]. This industry supports over 10 million jobs [43, 44], invests over $30 billion in R&D spending [45], and 72% of companies had positive free cash flow in the last year, with 86% reporting positive upstream earning [46]. This work includes a compliance graph within this sector as a means to showcase its application and utility for analyzing cost-savings and methodologies for following compliance mandates. This subsector is globally applicable, and has a wide range of focal points and scale that include upstream, midstream, and downstream related services and processes. Specifically, this work examines the processing, transportation, and storage of oil and

gas related products, byproducts, and intermediates as they relate to Occupational Safety and Health Administration (OSHA) regulations, and in particular, Standard 1910, Subpart H - Hazardous Materials [8]. In past years, the top 10 OSHA standard citations were from Standard 1910 [47]. From 2022 to 2023, specifically for Standard 1910 Subpart H, there were a total of 996 citations, 589 investigations, and a total imposed civil monetary fines of $4,995,005 across relevant North American Industry Classification System (NAICS) sectors [48]. Due to the applicability of OSHA Standard 1910 Subpart H to all Hazardous Material related activities of the oil and gas industry and relevant subsectors, the quantity of noncompliance complaints, and the total monetary collection as a result of noncompliance, this work generates and analyzes an OSHA 1910H compliance graph. This Section discusses the generation process, graph properties, unique features, and incurred challenges with this example application.

4.1 Network Properties, Data, and Violation Specifications

The OSHA 1910H example is centered an oil and gas company that processes, transports, and stores oil and gas related products, byproducts, and intermediates. This example models and analyzes their compliance standings to OSHA Standard 1910 Subpart H - Hazardous Materials over the course of 8 years. Since this is a federal regulation, specific guidelines and mandates are publicly accessible through the Occupational Safety and Health Administration. OSHA Standard 1910 Subpart H necessitates a range of requirements be met to ensure compliance, which include requirements for specific hazardous materials such as compressed gases, acetylene, flammable liquids, chemicals, and waste, among others. Compliance graph generator input files were created following the OSHA guidelines, and the properties for the generated OSHA compliance graph are listed below.

- Number of Nodes: 48,369
- Number of Edges: 408,330
- Number of Exploits: 32
- Number of Qualities: 109
- Number of Assets: 3
- Average Degree: 8.442

Properties and assumptions of the oil and gas company are listed below.

- The company has separate divisions for transportation, storage, and processing.
- The organization has an in-house Safety staff (that is **not** modeled).
- The company has an in-house fabrication/machining/manufacturing shop.
- The company has ownership of the vehicle transportation fleet.
- In addition to any imposed fines, failures or malfunctions can and/or will cause additional damages, such as:
  - Leakage or spillage.
  - Gaseous emissions.
  - Contamination.
  - Physical damage to company and/or non-company assets.
  - Burst pipes.
  - Schedule delays.

  - Violations in contracts.
- As part of, and in addition to, upholding OSHA 1910 Subpart H requirements, examples of other compliance standards include:
  - ASTM A 53/A 53M-06a into § 173.5b
  - CGA Pamphlet G-2.2 into § 173.315
  - Dwg. 106-6 into § 178.337-8
  - ASTM A 20/A 20M-93a into §§ 178.337-2; 179.102-4; 179.102-1; 179.102-17
  - ASTM A 302/A 302M-93 into § 179.100-7; 179.200-7; 179.220-7
  - Among others.
- Inspections include specific testing, such as:
  - Plastic Film Impact Resistance Testing.
  - Chlorine Flow Valve Removable Baskets.
  - Water in Anhydrous Ammonia.
  - Anhydrous Ammonia Hose pressure and burst pressures.
- Additional components modeled in this compliance graph include:
  - Ventiliation and exhaust systems.
  - Coatings, castings, and materials.
  - Transportation staff.
  - Bleeder valves, backflow check valves, and bin discharge gates.

For this example, multiple assets are implemented to capture and model their relationships individually, as well as to other assets. These assets include transportation, ventilation, and vessel assets. Each asset had its own set of qualities, and their own quality for measuring the progression of time. In order to prevent unnecessary state space exploration on unfeasible states caused by a deviation in time progression, a synchronous firing feature [38] in the generator tool was used. Various exploit locks and flags were also implemented to prevent diverting, duplicated branches of simultaneous exploit triggers. This was implemented through the use of precondition guarding, and was necessary since exploits could be fired through multiple conditions, but should only be fired once. Additionally, the problem space was able to be reduced through the use of combined events. Rather than having exploits or events contain single quality changes, events could be grouped to update multiple qualities simultaneously. This was implemented through inspection, assessment, or time-based events, which acted as a single point of action for all assessments, inspections, repairs, services, or any other event that would correct any violation and return the organization to a state of compliance. To further prevent divergence, all pre-defined events were also described using locks and flags, so the event (e.g. challenges with design scope, or improperly fabricated parts) would happen a single time at a specific point in the generation.

The data sourcing for the violation specifications and prior-knowledge network consisted of imposed civil monetary penalties for noncompliance, time closures for noncompliance, and implementation or mitigation costs to prevent a compliance violation. At the time of this release, the prior-knowledge network is undergoing additional formatting and feature work before its release. The prior-knowledge networks are intended to be added to the released dataset, and the initial work is described in this publication. The penalty structure as set by the Occupational Safety and Health Administration is defined as per Standard 1903.15 - Inspections, Citations, and Proposed Penalties [49]. These penalties are categorized by type of violation, which include willful violations, repeated violations, serious violations, other-than-serious violations, and posting requirement violation. Each of these categories has a defined maximum penalty, with some categories having

minimum requirements, and with some categories including units of time (e.g. monetary penalties per day). The prior-knowledge network was constructed around all publicly available sources, and contained additional detail about each exploit in the network. Damages, as relevant, were estimated in terms of costs of repairs, repeated fabrications, or other fines as necessary. No estimations were made regarding environmental damage, damages to animal or wildlife populations, or any other type of damages. For each exploit, the cost of occurrence was described. These costs were expressed as one-time monetary costs, recurring monetary costs and their rate of charge, and one-time time-commitment costs, recurring time-commitment costs and their rate of charge. For each exploit, possible mitigation schemes were described. Each exploit could have zero or many mitigation options. Each mitigation option described one-time monetary costs, recurring monetary costs and their rate of charge, and one-time time-commitment costs, recurring time-commitment costs and their rate of charge for preventing the exploit. For this example, most exploits had two mitigations. This will be described further in Section 4.2.

4.2 Objectives and Goals of the Network

The primary objective of this example is to highlight the usefulness of the analysis methods for preventing or mitigating larger, more catastrophic events or penalties. Many events or exploits would lead to further, repeated or increased damages. This example highlights the effectiveness of how investing in better policies, procedures, materials, and quality of components has substantial cost-saving benefits over time. This example network has unique properties not seen in the other example networks. This network includes cascading or repeated costs. If one (or multiple) components fall into a state of noncompliance, the resulting fines and damage costs increase. For the analysis of this work, this example showcases how a company could invest earlier on in a company project to maintain compliance and avoid cascading costs. This example also includes the ability to invest more time, rather than monetary investments. Most mitigatable exploits include at least two mitigations: one for including longer timeframes for inspections, testing, and quality control, and another for investing in better quality material, machinery, and staff investment. The latter option requires minimal time cost, but has a greater monetary cost. The former requires minimal monetary cost, but a greater time cost. This allows for the analysis to offer more robust correction schemes that can utilize both the monetary and time budgets to minimize and correct compliance violations.

5 Future Works

Due to the novelty of compliance graphs, there are multiple avenues available for future research investigations. This work provided the compliance graph input and output files for the RAGE Attack Graph Engine. Future works could include the output compliance graphs when using these input files for alternative generator tools. The output compliance graphs could undergo a comparison to identify or uncover information that could assist in future analysis works. The compliance graph analysis space would also benefit both from a broader range of compliance graphs, and compliance graphs with finer detail. Though this work implemented a compliance graph for OSHA 1910H, the various standards and guidelines that fit under this regulation (such as various ASTM standards) possess more detail and information than was incorporated in this example. Including full, in-depth input files that describe all details of a regulation would provide researchers the tools to conduct a thorough investigation into compliance graph analysis. Future works are likely to include additional input files that describe potential mitigation or solution opportunities for known

states of noncompliance. These input files would not be included as part of the generation process, but could be used to further describe the known nodes and edges of a given compliance graph. These files could indicate transitional probabilities or weights of edges, the fines or penalties when states of noncompliance are identified, or the costs of repair or replacement of components.

6 Conclusion

This work presented the generation process of three distinct compliance graphs across three unique industries. The generation of each of these example graphs was described in each respective Section along with the data sourcing techniques. The output files of these graphs have been publicly released, along with their input data files. This work aims to provide a starting foundation for compliance graph analysis through example cases that can be explored and improved upon. The automobile maintenance network provides a compliance graph that describes the state of a personal vehicle over a period of time as it relates to the recommended maintenance schedule provided by the vehicle manufacturer. The healthcare network provides a compliance graph that describes the state of an urgent care clinic as it strives to maintain compliance to HIPAA. The oil and gas network provides a compliance graph that describes the state of an oil and gas company as it transports, stores, and processes hazardous material and works to maintain compliance to OSHA 1910H. Each of these example networks contains unique properties that highlights edge cases and insightful information about each industry and various compliance and noncompliance information.

References

[1] K. Zenitani, "Attack graph analysis: An explanatory guide," *Computers & Security*, vol. 126, p. 103081, 2023.
[2] J. Hale, P. Hawrylak, and M. Papa, "Compliance Method for a Cyber-Physical System." U.S. Patent Number 9,471,789, Oct. 18, 2016.
[3] N. Schrick and P. Hawrylak, *Compliance Graph Generation Techniques and Parallel Computing Implementations Using Message-Passing Interfaces*. MS thesis, The University of Tulsa, Tulsa, OK, 2022.
[4] "Financial Crimes Enforcement Network, Title 31 U.S.C. 310," 2010. Available: https://www.govinfo.gov/content/pkg/USCODE-2010-title31/html/USCODE-2010-title31-subtitleI-chap3-subchapI-sec310.htm.
[5] Food and Drug Administration, "Quality system regulations," 1996. Federal Register: Volume 61, Number 195. 1996 [Online]. Available: https://www.fda.gov/science-research/clinical-trials-and-human-subject-protection/quality-system-regulations.
[6] Federal Energy Regulatory Commission, "Critical infrastructure protection reliability standard cip," 2020. 85 FR 8161. 2020 [Online]. Available: https://www.federalregister.gov/documents/2020/02/13/2020-02173/critical-infrastructure-protection-reliability-standard-cip-012-1-cyber-security-communications.
[7] "Health Insurance Portability and Accountability Act of 1996." Pub. L. No. 104-191. 1996 [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.
[8] Occupational Safety and Health Administration, "Standard 1910 Subpart H Hazardous Materials," Last Amended 2024 via Code of Federal Regulations Title 29.
[9] N. Schrick and P. Hawrylak, "Compliance graph network files and exploit models," July 2024.
[10] K. Cook, "RAGE: The Rage Attack Graph Engine," Master's thesis, The University of Tulsa, 2018.
[11] International Trade Administration, U.S. Department of Commerce, "Automotive Industry," August 2021. [Online]. Available: https://www.trade.gov/selectusa-automotive-industry.
[12] International Trade Administration, U.S. Department of Commerce, "Foreign Direct Investment (FDI): Automotive," August 2021. [Online]. Available: https://www.trade.gov/sites/default/files/2021-09/Automotive%20-%20FINAL.pdf.
[13] U.S. Bureau of Economic Analysis, "Industry Factsheet: Transportation and Warehousing," 2023. [Online]. Available: https://apps.bea.gov/industry/factsheet/factsheet.html#48TW.
[14] U.S. Bureau of Economic Analysis, "Value Added by Industry," 2023-12-21.

[15] U.S. Bureau of Economic Analysis, "Gross Output by Industry," 2023-12-21.
[16] Singh, A, and Singh, S., "Automotive Repair and Maintenance Service Market Size," Feb. 2024. [Online]. Available: https://www.gminsights.com/industry-analysis/automotive-repair-maintenance-services-market.
[17] Toyota Motor Sales, U.S.A., Inc., "Downloadable Manuals." [Online]. Available: https://www.toyota.com/owners/warranty-owners-manuals/.
[18] U.S. Department of Energy, "Alternative Fuels Data Center." [Online]. Available: https://afdc.energy.gov/data/categories/driving-patterns.
[19] National Transportation Statistics Datasets, "United States Department of Transportation Bureau of Transportation Statistics." [Online]. Available: https://www.bts.gov/product/national-transportation-statistics.
[20] U.S. Department of Transportation Federal Highway Administration, "Highway Statistics Series." [Online]. Available: https://www.fhwa.dot.gov/policyinformation/statistics.cfm.
[21] Preston, B., "Car Brands and Models That Can Save You Money Over Time," 2023-04-02. [Online]. Available: https://www.consumerreports.org/cars/car-repair-maintenance/car-brands-and-models-that-can-save-you-money-over-time-a9081677414.
[22] AAA, "Planning for Auto Maintenance and Repair Costs." [Online]. Available: https://www.aaa.com/autorepair/articles/planning-for-auto-maintenance-and-repair-costs (visited on Feb. 25, 2024.).
[23] Farmers Insurance, "Auto Service and Repair Shop Insurance." [Online]. Available: https://www.farmers.com/business/industry/auto-service-repair/ (visited on Feb. 25, 2024.).
[24] AAA, "Your Driving Costs," 2020-12-09. [Online]. Available: https://newsroom.aaa.com/wp-content/uploads/2020/12/Your-Driving-Costs-2020-Fact-Sheet-FINAL-12-9-20-2.pdf.
[25] Centers for Medicare & Medicaid Services, "NHE Fact Sheet," 2022. [Online]. Available: https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/nhe-fact-sheet.
[26] The World Bank, "Current Health Expenditure (% of GDP)," 2023-04-07. [Online]. Available: https://data.worldbank.org/indicator/SH.XPD.CHEX.GD.ZS?name_desc =true&locations=US.
[27] Organisation for Economic Co-operation and Development, "OECD Health Statistics 2023," 2023. [Online]. Available: https://www.oecd.org/health/health-data.htm.
[28] Centers for Disease Control and Preventation, "Health Expenditures," 2019. [Online]. Available: https://www.cdc.gov/nchs/fastats/health-expenditures.htm.
[29] Bureau of Economic Analysis, "New Health Care Statistics for First Year of COVID-19 Pandemic," 2023-02-10. [Online]. Available: https://www.bea.gov/news/blog/2023-02-10/new-health-care-statistics-first-year-covid-19-pandemic.
[30] Bureau of Economic Analysis, "Experimental Data Map Health Care Estimates in GDP to Centers for Medicare & Medicaid Framework," 2023-09-25. [Online]. Available: https://www.bea.gov/news/blog/2023-09-25/experimental-data-map-health-care-estimates-gdp-centers-medicare-medicaid.
[31] National Center for Science and Engineering Statistics, "R&D; Most Pharmaceutical R&D Focused on Biotechnology," 2018. [Online]. Available: https://ncses.nsf.gov/pubs/nsf21316.
[32] Congressional Budget Office, "Research and Development in the Pharmaceutical Industry," April 2021. [Online]. Available: https://www.cbo.gov/publication/57126.
[33] American Hospital Association, "Fast Facts on U.S. Hospitals, 2024," 2024. [Online]. Available: https://www.aha.org/statistics/fast-facts-us-hospitals.
[34] Definitive Healthcare, "Healthcare Insights," 2023-08-22. [Online]. Available: https://www.definitivehc.com/resources/healthcare-insights/urgent-care-clinics-us.
[35] Association of American Medical Colleges, "Workforce Data," 2019. [Online]. Available: https://www.aamc.org/data-reports/workforce/data/active-physicians-us-doctor-medicine-us-md-degree-specialty-2019.
[36] U.S. Department of Health and Human Services, "Compliance Enforcement Data," 2024-01-31. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html.
[37] U.S. Department of Health and Human Services, "Enforcement Highlights," 2024-01-31. [Online]. Available:https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.
[38] N. L. Schrick and P. J. Hawrylak, "State space explosion mitigation for large-scale attack and compliance graphs using synchronous exploit firing," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 147–157, 2023.
[39] U.S. Department of Health and Human Services, "Resolution Agreements," 2024-02-06. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.
[40] U.S. Department of Health and Human Services, "Reports to Congress on Privacy Rule and Security Rule Compliance," 2022. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html.

[41] U.S. Department of Health and Human Services, "HIPAA Privacy, Security, and Breach Notification Audit Program," 2020. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.
[42] U.S. Department of Health and Human Services, "Case Examples," 2023-11-01. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html.
[43] United States Census Bureau, "Oil & Natural Gas," 2019. [Online]. Available: https://www.census.gov/history/pdf/api-082021.pdf.
[44] U.S. Department of Energy, "Economic Impact of Oil & Gas," 2020. [Online]. Available: https://www.energy.gov/articles/economic-impact-oil-and-gas.
[45] International Energy Agency, "R&D Technology Innovation," 2020. [Online]. Available: https://www.iea.org/reports/world-energy-investment-2020/rd-and-technology-innovation.
[46] U.S. Energy Information Administration, "Financial Review of the Global Oil and Natural Gas Industry: Third-Quarter 2023," December 2023. [Online]. Available: https://www.eia.gov/finance/review/pdf/3Q2023%20Financial%20Review.pdf.
[47] Smart, S.J., "Keeping Oil and Gas Workers Safe and Avoiding Costly Penalties," June 2015. [Online]. Available: https://ohsonline.com/Articles/2015/06/01/Keeping-Oil-and-Gas-Workers-Safe-and-Avoiding-Costly-Penalties.aspx.
[48] U.S. Department of Labor, Occupational Safety and Health Administration, "Industry Profile for an OSHA Standard Results," 2023. [Online]. Available: https://www.osha.gov/ords/imis/industryprofile.html.
[49] U.S. Department of Labor, Occupational Safety and Health Administration, "Standard Number 1903.15 - Proposed Penalties," 2024-01-15. [Online]. Available: https://www.osha.gov/laws-regs/regulations/standardnumber/1903/1903.15.

Received 31 October 2024; revised XXXXXX; accepted XXXXXX