2019

A complex structure representation of the US critical infrastructure protection program based on the Zachman Framework

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Unal Tatar
University at Albany, State University of New York, utatar@albany.edu

Polinpapilinho F. Katina
University of South Carolina - Upstate, pkatina@uscupstate.edu

Andy Igonor
Franklin University, andy.igonor@franklin.edu

Recommended Citation

Karabacak, B., Tatar, U., Katina, P. F., & Igonor, A. (2019). A complex structure representation of the US critical infrastructure protection program based on the Zachman Framework. *International Journal of System of Systems Engineering, 9* (3), 221-234. https://doi.org/10.1504/IJSSE.2019.102869

A complex structure representation of the US critical infrastructure protection program based on the Zachman framework

Unal Tatar*

College of Emergency Preparedness,
Homeland Security and Cybersecurity,
University at Albany – SUNY,
Albany, NY 12222, USA
Email: utatar@albany.edu
*Corresponding author

Bilge Karabacak

Ross College of Business,
Franklin University,
Columbus, OH 43215, USA
Email: bilge.karabacak@franklin.edu

Polinpapilinho F. Katina

Department of Informatics and Engineering Systems,
University of South Carolina Upstate,
Spartanburg, SC 29303, USA
Email: pkatina@uscupstate.edu

Andy Igonor

Ross College of Business,
Franklin University,
Columbus, OH 43215, USA
Email: andy.igonor@franklin.edu

Abstract: Critical infrastructures are vital assets for public safety, economic welfare or national security of countries. The importance of critical infrastructures necessitates state-level coordination of security efforts based on some rigid policies, strategies, and procedures. This hierarchical set of rules is collectively referred to as the critical infrastructure protection program (CIPP). As the pioneer of CIPP, the USA has a very complex program in which partners and stakeholders have multiple and varied interacting roles and responsibilities. The complexity of roles and interactions creates a need to make a representation of these complex structures by using intuitive tools. The Zachman framework is such a tool that provides a formal and structured way of viewing and defining a complex enterprise. It is represented by a 6×6 matrix with rows defining stakeholders and columns defining underlying interrogatives. In this article, a proof-of-concept study is performed to represent

the US CIPP using the Zachman framework. The proof-of-concept study showed that the Zachman framework could be beneficial in overcoming challenges of a CIPP program which can be regarded as a complex enterprise.

Keywords: critical infrastructure protection program; CIPP; cyber security; roles and responsibilities; stakeholders; enterprise architecture; Zachman framework; system of systems.

Reference to this paper should be made as follows: Tatar, U., Karabacak, B., Katina, P.F. and Igonor, A. (2019) 'A complex structure representation of the US critical infrastructure protection program based on the Zachman framework', *Int. J. System of Systems Engineering*, Vol. 9, No. 3, pp.221–234.

Biographical notes: Unal Tatar is an Assistant Professor of Cybersecurity at the College of Emergency Preparedness, Homeland Security, and Cybersecurity. He worked as a principal cybersecurity researcher in government and industry for 10+ years. He is the former coordinator of the National Computer Emergency Response Team of Turkey. He worked in cyber risk assessment projects in various critical infrastructure sectors as a researcher and project manager. He holds a BSc degree in Computer Engineering, an MS degree in Cryptography. His PhD degree is in Engineering Management and Systems Engineering from Old Dominion University, Norfolk, VA. He is the Director of the NATO Advanced Research Workshop on a Framework for a Military Cyber Defense Strategy. His main topics of interest are information/cybersecurity risk management, cyber resiliency, economics of cybersecurity, cyber insurance, blockchain, and IoT security.

Bilge Karabacak is a Lead Faculty at Franklin University. He received his PhD in Information Systems from Graduate School of Informatics at Middle East Technical University, MS degree in Computer Engineering from Gebze Technical University and BS in Electrical Engineering from Bilkent University. His research topics are information security risk analysis, governance, compliance, critical infrastructure protection, cyber regulations, cybersecurity maturity models and IoT security.

Polinpapilinho F. Katina currently serves as an Assistant Professor in the Department of Informatics and Engineering Systems at the University of South Carolina Upstate (Spartanburg, South Carolina). He previously served as a Postdoctoral Researcher at National Centers for System of Systems Engineering (NCSOSE) at Old Dominion University (Norfolk, Virginia) and Adjunct Professor in the Department of Engineering and Technology, Embry-Riddle Aeronautical University – the Worldwide Campus. His profile includes more than 100 peer-review journal articles, conference papers, book chapters and books. He has teaching/research interests in complex system governance, critical infrastructure systems, decision analysis, engineering management, manufacturing systems, resilient systems, system of systems engineering, system pathology, systems engineering, and systems science. He holds a PhD in Engineering Management and Systems Engineering from Old Dominion University and received additional training from Politecnico di Milano (Milan, Italy). He is a founding board member of the International Society for Systems Pathology (Claremont, California).

Andy Igonor is an information technology and security professional with over 20 years of academic and professional experience working across different industries including healthcare, finance, and telecommunications. His experience includes using his knowledge of security tools, techniques, and best practices to help create and deploy solutions that protect systems and information assets, especially for clients in healthcare. He worked on major projects with the Brandon Healthcare Trust, UK; Health Canada; the Physician Office System Program (POSP), Alberta, Canada; and the Business Development Bank of Canada, in the areas of security threat and risk assessments of cloud-deployed solutions, privacy impact assessments, and the development of security architectures. He has also been involved in the selection and implementation of electronic health records (EHR) systems, as well as enterprise resource planning systems including SAP, Microsoft Dynamics (GP, NAV), SAGE, Exact, etc. for large, small and medium-sized clients.

1 Introduction

Critical infrastructures are vital assets for public safety, economic welfare or national security of countries. Energy, telecommunications, finance, security services, health systems, transportation, and water management are prominent examples of critical sectors which include many critical infrastructures.

The utilisation of cyber systems to monitor and control critical infrastructures efficiently and cost-effectively have been increasing with every passing day. For example, modern and connected information technologies are used in controlling energy and water management systems in contrary to isolated legacy systems of the past. Smart grids, smart transportation systems, and remotely controllable local gas distribution systems have been emerging as vital parts of modern society. Some critical infrastructures are entirely dependent on conventional cyber systems. For instance, today's banking and finance infrastructure substantially depends on information technologies. Telecommunication infrastructure is wholly composed of cyber systems. Because of new service models like cloud computing, the internet can be regarded as critical infrastructure (Beltran and Fontenay, 2005). The 2007 attack on Estonia networks demonstrated how much the well-being of a country depends on internet infrastructure (Kozlowski, 2014; Tatar et al., 2014).

Critical infrastructures must be protected in conformity with some specific policies because of the attack potential of these threats especially today's cyber threats. That is why most of the developed countries have national critical infrastructure protection programs (CIPP). CIPP is a national and coordinated effort created to protect critical infrastructures from both cyber and physical threats (Dunn and Wigert, 2004). A typical CIPP includes all responsible and related stakeholders from critical infrastructure operators, government (federal and local), the private sector, academia, and non-profit organisations.

When one examines the CIPP of several countries, it can be seen that there are some critical challenges almost every CIPP encounters. Firstly, the vast number of stakeholders is a common challenge for CIPPs. Critical infrastructure protection is not only the result of the contributions of all stakeholders but also the interactions of them; these stakeholders have to cooperate to achieve their goals. The multitude of stakeholders and the vast amount of stakeholder actions are the basis of the complex relationships and interdependencies among critical infrastructures (Idaho National Laboratory, 2006). Another challenge is the high ratio of the private sector ownership of critical infrastructures. Market-oriented settings make government intervention and regulatory actions challenging to employ (Karabacak et al., 2016).

Rinaldi et al. (2001) appraise multiple infrastructures as a system of systems. In another article, Rinaldi (2004) asserts that "understanding the operational characteristics of and providing a sufficient level of security for these infrastructures requires a system-of-systems perspective, given their interdependencies". According to Walters et al. (2014), "complex systems are characterized by many autonomous and diverse, interrelated components, tightly coupled through many interconnections". They discuss the implications of the integration of system of systems engineering and enterprise architecture. Authors point out the contribution of the integration as the enhanced governance of complex systems. Carter et al. (2016) also discuss enterprise architecture view of complex system governance. They discuss the increasing complexity of the system of systems contexts and explore the governance architecture concept. According to the DoD Guide for Systems Engineering of Systems of Systems, "a system of systems is a collection of systems, each capable of independent operation, that interoperate together to achieve additional desired capabilities" (Department of Defense, 2008). All critical infrastructures in every sector in a country can be regarded as an enormous system of systems. Because each critical infrastructure is capable of independent operation and those infrastructures interoperate together to achieve a prosperous nation. Therefore, a CIPP can be regarded as one of the essential means to manage the system of systems of critical infrastructures. Authors reviewed and summarised the articles that formulate the system of systems approach for interdependent critical infrastructures in the literature review section.

At this point, the Zachman framework – as a fundamental structure for enterprise architecture – can be used to represent the CIPP of a country in an insightful way. First of all, an enterprise is a collection of organisations or business units that share a common set of goals. CIPP can intuitively be regarded as an enterprise with many stakeholders with the goal of securing infrastructures and the country as a whole. The CIPP of the USA is a very complex and dynamic enterprise. Because it is complex and changing, it needs to be written formally. Architecture is a formal way of describing a system and guiding its implementation and also the key to dealing with change and complexity (Zachman, 2003). The Zachman framework is a comprehensive and well-defined matrix tool for Enterprise Architecture. The Zachman framework can also be defined as "a fundamental structure for Enterprise Architecture which provides a formal and structured way of viewing and defining an enterprise" (Sowa and Zachman, 1992). It is a 6×6 matrix with rows representing different points of view of an enterprise and the columns representing underlying interrogatives. Romero and Vernadat point out the shift from traditional enterprise architecture to digital architecture, namely next-generation enterprise architecture, which includes the latest digital technologies (Romero and Vernadat, 2016). In the next-generation enterprise architecture, cross-business processes can be quickly

modified, and these changes should not be regarded as exceptions, but normality. Zachman framework can be used to handle the rapid changes in enterprises.

In this paper, a proof of concept study has been made with the participation of practitioners in which the US CIPP has been represented partly using the Zachman framework. The purpose of the study is not to represent the whole CIPP of the USA using the Zachman framework, as this can be a topic of a more comprehensive case study. Instead, the purpose of the study is to show the suitability of the Zachman framework for the representation of complex enterprise architectures like CIPP and the development of a proof-of-concept study.

Section 2 is dedicated to a literature review in which academic studies that embrace a combined study of the Zachman framework and information security are summarised. Section 3 delineates challenges associated with the protection of critical infrastructures. In Section 4, both the problem statement and the motivation for this study are shared with the reader. The detailed information about the matrix, the description of its rows, columns, and the rules of formation are given in the Section 5. Section 6 shows a proof-of-concept representation of the US CIPP based on the Zachman framework. Section 7 is dedicated to discussions and conclusions.

2 Literature review

Various studies propose the use of an enterprise architecture framework for modelling security features of an enterprise. In this section, seven academic studies that propose the use of the Zachman framework or enterprise architecture in the information security area are reviewed. The purpose of the studies changes from ensuring better coordination within the enterprise to increasing efficiency.

Pulkkinen et al. (2007) use enterprise architecture as a means of "comprehensive and coordinated planning and management of corporate ICT and security infrastructure". This study uses enterprise architecture to plan security architecture in which technological solutions are developed according to business goals. The authors performed a case study in a real organisation. The security-related decisions are mapped into a 12-cell matrix so that an enterprise architecture context is created. The rows of the matrix show enterprise, domain and systems levels of the organisation in the case study – columns of the matrix show business, information, applications and technology architectures.

Ertaul and Sudarsanam (2005) show how the Zachman framework can be used in defining, designing and creating tools for effectively securing an enterprise. The authors fill out the 6×6 matrix to create a generic model that shows the generalised plan for a secured enterprise. The authors use a new column named 'external requirements and constraints' in place of the 'motivation/why' column that is present in the original version of the Zachman framework.

Rosa uses the Zachman framework to evaluate the readiness of an IT infrastructure of a real organisation (Rosa, 2008). The author audits the organisation and proposes recommendations, firstly. Secondly, the author places the recommendations to the matrix of the Zachman framework, so that coverage of the recommendations can be seen in the perspective of the Zachman framework. Eleven out of 36 cells of the matrix are filled by the recommendations. The first column (what) and fifth row (sub-contractor view) all have empty cells. According to the author, the representation of recommendations with

the Zachman framework is useful and sufficient in determining countermeasures of business continuity.

Feltus et al. (2014) propose an architecture for SCADA information systems that are used to control and monitor critical infrastructures. The authors use ArchiMate enterprise architecture model to model "SCADA components to enrich SCADA component collaborations and the description of their behavior in the cyber policy". The authors posit that current enterprise architecture models such as TOGAF, ArchiMate, and Zachman framework consider only human actors at the business level. They claim that beyond human actors, software autonomous entities have to be taken into consideration for the distribution of security policies because of the rising security requirements for the management of heterogeneous and distributed architecture. It is also posited that intelligent software items manage complex systems.

Oda et al. (2009) review three enterprise information security architecture frameworks by taking security integration features into account. The reviewed frameworks are the Sherwood Applied Business Security Architecture (SABSA), Gartner EISA framework, and Zachman framework (Oda et al., 2009). These authors emphasise that 'information security architecture' is a subset of enterprise architecture which is focused on aligning information security with business strategy. They provide some information on architecture frameworks saying that SABSA focused on business to security and based on the Zachman framework. EISA provides details on how security is incorporated into the enterprise architecture. In this regard, the Zachman framework is generic compared to the SABSA and EISA. However, it can be used for security architecture modelling. The authors extract the common and different features of the frameworks. Because of the space constraints, it is suggested to refer to the article for further details. The authors also compare the enterprise architecture of Oakland University with the reviewed frameworks and develop some suggestions for the university.

Ekstedt and Sommestad (2009) claim that current architectural languages are not sufficient for security analyses. These authors present three reasons for insufficient support of architectural frameworks for security analyses. Firstly, they lack enough details to provide the information required for the analyses. Secondly, they do not propose attributes systematically. Thirdly, many frameworks do not contain classes to model control systems. In their paper, authors combine security theory and architecture models and propose abstract models that are built from attack and defence tree.

Urbaczewski and Mrdalj (2006) compare five enterprise architecture frameworks in terms of views/perspective, abstractions, and system development lifecycle phases. The paper is one of the most comprehensive and detailed comparisons of the enterprise architecture frameworks in the literature. The authors conclude that the Zachman framework is the most comprehensive framework as it uses many viewpoints related to different aspects whereas other frameworks represent a small number of viewpoints and aspects.

Two authors of the article proposed a roles and responsibilities matrix that was aimed at improving national cybersecurity governance (Tatar et al., 2016). In this study, authors created 6 × 3 matrices in which the roles and responsibilities are determined by taking incident timeline (e.g., before, during and after a cyber incident) and critical actions (e.g., detection and response) into account. Although the proposed matrix is not within the scope of enterprise architecture, it can be considered as a demonstration of an enterprise by taking certain constraints into account.

It can be seen that the Zachman framework has been applied successfully for the security modelling of the enterprise. The enterprises that are considered in the reviewed studies are standalone organisations. No study attempts to model a complex enterprise that is composed of many different types of organisations like CIPP. This study will be the first study of its kind.

Authors also reviewed the articles that use the system of systems approach to analyse critical infrastructure, and to improve the resiliency of the infrastructures (Eusgeld et al., 2011; Kröger, 2008; Little, 2003; Thacker et al., 2017; Tolone et al., 2009). All of these studies focus on the interdependencies of critical infrastructures. Authors of these articles consider interdependent critical infrastructures as examples of a system of systems and propose models to analyse cascading failures or prevent the propagation of the failures among critical infrastructures. All of the articles also concentrate on the technical aspects of critical infrastructures. As an example, Eusgeld et al. (2011) model the interdependencies between supervisory control and data acquisition (SCADA) systems among different infrastructures and experiment the failure propagation due to the single or multiple failures in SCADA systems. Among those articles, Kröger (2008) emphasises the societal and institutional aspects of the critical infrastructures in addition to system-related, technological, and natural aspects. At this point, it is worth mentioning a software called Athena. The development is sponsored by Air Force Research Laboratory and funded by DARPA and USSTRATCOM later on. Athena is an analysis and modelling software that is designed to actors, concepts and physical entities as a system of systems. Athena has the capability of "merging various political, military, economic, social, information, and infrastructure models and their associated cross dependencies" (Idaho National Laboratory, 2006). It is used in the assessment of global failures such as hurricane impact analysis and natural disaster planning exercises. Although the academic studies that combine the concepts of the system of systems approach and critical infrastructures mainly focus on the technical aspects of the critical infrastructures, similar models can be devised at the organisational level. The proposed Zachman framework in this article can be used as a basis for the studies that aim to model the organisational-level relationships and interdependencies of the critical infrastructures.

3 Challenges of the critical infrastructure protection programs

The concept of critical infrastructure protection is an evolving and broad topic. The dynamic nature of cyber threats and the proliferation of the information technologies among all of the sectors from agriculture to communication contribute to both the evolution of the CIPP over the years and to the broadness of the topic. This evolution and broadness pave the way of the challenges inherent in the CIPPs of these countries. When the CIPP of the USA is taken into account, the following prominent challenges can be listed.

In the USA, critical infrastructures are mostly operated by the private sector (de Bruijne and van Eeten, 2007). The focus of the private sector in using cyber systems is mostly to ensure efficient and cost-effective management of critical infrastructures. Because critical infrastructure protection is a subset of national security (Klimburg,

2012), it is important to say that, the security of the private sector is closely related to national security in the digital era (Andress, 2003). Therefore, other constraints like security and resiliency apart from the constraints like efficiency and cost should be taken into account in controlling and monitoring the infrastructures. This situation causes tension between private sector and government. While government officials urge the regulations as an essential gadget for critical infrastructure protection, private sector asserts the regulations as the obstacles before the innovations (Karabacak et al., 2016), (Orlowski, 2001). As an example, the Cybersecurity Act of 2012 failed to pass the US Senate as the result of this tension, although White House endorsed it (Kelly, 2012).

Secondly, one of the main characteristics of the CIPPs of the countries is the existence of many stakeholders that have to cooperate to achieve the goals. The reality of the multitude of stakeholders also applies to the USA. Some factors result in the existence of a vast number of stakeholders. First of all, cybersecurity has many dimensions including fighting against cybercrime, cyber military, cyber diplomacy, and cyber intelligence (Klimburg, 2012) – the presence of these dimensions necessities the cooperation of the government actors related with these dimensions. Secondly, critical infrastructures are mostly operated by the private sector as said in the first paragraph. Therefore, the private sector has to be one of the most important stakeholders. Thirdly, developed countries have been establishing new government agencies for the protection of critical infrastructures. For example, the Department of Homeland Security of the USA was established after the 9/11 attacks. These new organisations introduce new stakeholders as well. Finally, the technical aspects of cybersecurity introduce new stakeholders to the CIPP. For example, activities like research and development and capacity building are very vital aspects of the CIPPs. The multitude of stakeholders is also the basis of the complex relationships and interdependencies among stakeholders. Critical infrastructure protection is not only the result of the contributions of all stakeholders but also the interactions of them. The isolated efforts of the stakeholders will not be useful no matter how excellent these efforts are. At this point, the problems with information sharing and cooperation among critical sectors and critical infrastructures come as a challenge. Building a partnership between the private sector and government is a challenge as well. That is why the key theme of the national infrastructure protection plan (NIPP) is building a partnership. NIPP is the central document of the current CIPP of the USA (Department of Homeland Security, 2013). NIPP contains the complete list of the stakeholders and their roles and responsibilities. It also contains the collaboration and cooperation requirements to achieve secure and resilient infrastructures.

As an example, there are sixteen critical sectors in the USA (The White House, 2013). There are thousands of critical infrastructures under these sectors. These infrastructures have different size, cultures, geographic locations, objectives. Therefore, these infrastructures have different views and practices for protection from cyber threats. Therefore, it is not easy to unite these organisations under a single CIPP (Klimburg, 2012; Canada, 2009). Because there are many stakeholders, associated roles and responsibilities and also interdependencies among both infrastructures and those stakeholders, it is difficult to comprehend the critical infrastructure protection efforts of the USA fully.

4 Problem statement and motivation

When the CIPP programs of the countries are examined, it is seen that there are many documents from a policy level to a tactical level. These documents include many stakeholders written in a flat (non-hierarchical) way and a vast number of interdependent roles and responsibilities. There is a need for an enterprise-level modelling tool to represent a CIPP. Authors claim that the Zachman framework can be used to represent CIPP of a country comprehensively. The use of the Zachman framework can also help in overcoming the challenges mentioned above. Because the rows of the Zachman framework make clear distinctions for owner, designer and implementers. It also helps to determine the scope of the enterprise. Zachman framework also helps in analysing a specific perspective in terms of six interrogatives. Therefore, almost every aspect of a perspective is analysed.

Secondly, it is essential to state that the results of the literature review have shown that the Zachman framework can be applied to the complex enterprises that deal with cybersecurity cases. This paper goes a step further. Authors represent the national CIPP of the USA by using the Zachman framework. The program of the USA has many participants including different federal and state-level organisations, private sectors, non-profit organisations, and academia. Consequently, this paper is the first attempt of the representation of a complex enterprise that is composed of many different organisations using the Zachman framework.

5 Basics of Zachman framework

The originator of the Zachman framework is John H. Zachman, who is the early pioneer of the enterprise architecture concept (Zachman, 2009). Enterprise architecture is a discipline in which the representation of the enterprise is performed for the successful development and execution of strategy (The Federation of Enterprise Architecture Professional Organizations, 2013; Gartner IT Glossary, 2016).

Zachman framework is a two-dimensional classification schema that reflects the intersection between two traditional classifications. Columns of the matrix are six interrogatives, which include the what, how, where, who, when, and why. The first column is a material description. It is all about the things that form the structure. The second column is a functional description. It is about the transformation and the processes. The third column is the spatial description. It is all about flow and the locations. The fourth column is the operational description. It is about operations and the people/organisations performing those operations. The fifth column is the timing description. It is about dynamics and events. The sixth column is the motivation description. It is about motivation and strategies.

Each row in the matrix represents a holistic and unique view of the enterprise from a particular perspective. The first row reflects an executive perspective; otherwise the planner's view. It is all about contextual scope. The second row represents the business management perspective. It is the owner's view. It is all about a conceptual business

model. The third row reflects the architect perspective. It is the designer's view. It is all about logical system model. The fourth row reflects the engineering perspective. It is the builder's view. It is all about physical technology model. The fifth row reflects technician perspective. It is the subcontractor's view. It is also called the out-of-context perspective. The sixth row reflects functioning enterprise, the result of the architectural process. It is not architecture, but it completes the architectural picture (Zachman, 2003). Second, third and fourth rows are called principal rows. First and fifth rows can be named as additional perspectives. The sixth row is a physical manifestation of the enterprise, not a representation (Zachman, 2003).

There are seven strict rules when filling out a matrix for an enterprise. Firstly, new columns should not be added to the matrix. The only flexible thing with columns and rows is the sequence of the columns. Columns can be interchangeable. Secondly, each column has a simple generic model. It means that each column describes a single independent variable for an enterprise. Thirdly, each cell model specialises in its column's generic model. It implies that the level of detail is a function of a cell, not a column. Fourthly, each shell should be unique. Fifthly, diagonal relationships should not be created between cells. Every cell is related to every other cell in a row. Every cell is related to the cell above and below in a column. Sixthly, the names of the rows and columns should not be changed. Finally, the logic of the framework is generic and recursive.

6 Proof of concept representation of CIPP with Zachman framework

Table 1 shows a proof-of-concept representation of the CIPP of the USA in the 6×6 matrix of the Zachman framework. The aim of the representation is not to show every aspect of the CIPP in a matrix. Instead, the Zachman framework provided an overview of the CIPP concisely. Before preparing the matrix, the federal documents of the USA regarding CIPP are reviewed. Among these documents, National Cyber Incident Response Plan, PPD-21 and NIPP were the most useful documents, because these documents are comprehensive, that is, that they contain most of the stakeholders and associated roles and responsibilities (Department of Homeland Security, 2013, 2016; The White House, 2013). for business management, architect, and engineer perspectives, extra rows are created for each organisation added to the perspective to represent the interrogatives of the organisations separately.

The CIPP program of the USA has many stakeholders with critical roles and responsibilities. The Zachman framework provided the opportunity of distinguishing different layers of roles and responsibilities. One may not realise the different layers of responsibilities when s/he reads the NIPP and eventually may get confused with many roles and responsibilities. With the help of the Zachman framework representation, not only primary layers came in view but also one can see which of the stakeholders are clustered in certain levels. Another advantage of the matrix is that it shows the fundamental interdependencies of the CIPP. In order to see the dependencies, one can examine the second column. In this column, there are sentences on how specific tasks are succeeded through the help of collaboration and cooperation.

Table 1 Representation of the CIPP of the USA

	What	*How*	*Where*	*Who*	*When*	*Why*
Executive perspective	Maintain and update critical infrastructure protection program and NIPP	By using statues, executive orders, presidential directives	Both in cyberspace and physical world	Department of Homeland Security	Before, during and after cyber incidents	For the prosperity of the USA
Business management perspective	Strategic guidance audit	By obeying Presidential Policy Directive – 21 and Executive Order 13636	Critical sector(s).	Sector-specific agencies	Day-to-day federal interface	For a natural unity of effort To implement its knowledge and specialised expertise about its sector
	Risk management	By coordinating overall federal effort		NIST		
Architect perspective	Coordination, collaboration, partnership		Federal government systems	National Cybersecurity and Communications Integration Center (NCCIC)	During incident response	To coordinate the Federal Government's asset response
	Coordination, collaboration, partnership	By partnering 20 agencies from across law enforcement, the intelligence community, and the Department of Defense/by collaborating international and private sector partners	Federal government systems	National Cyber Investigative Joint Task Force (NCIJTF) – Hosted by FBI	During the cyber terrorism, espionage, financial fraud, and identity theft incidents	To coordinate the Federal Government's threat response
Engineer perspective	Securely control and monitor critical infrastructures	The federal government provides information about risk environment	Critical infrastructures, SCADA systems, ISC systems	Critical infrastructure owners and operators	Throughout all lifecycle of the infrastructure	To prevent and detect cyber threats, to make Cis resilient
	Training, threat analysis, digital forensics	By supporting law enforcement, counterintelligence, information assurance, network defence, and critical infrastructure protection communities	Federal government	Department of Defense Cyber Crime Center (DC3)	During the national cyber incident response	To support federal agency mission partners by providing analytical and technical capabilities
	Offensive measures	By managing both the threat and asset responses	US Military and Department of Defense	US Cyber Command (USCYBERCOM) Joint Operations Center (JOC)	During incidents	For deterrence
Technician perspective	Security hardenings FISMA, HIPAA, GLBA, NERC requirements (compliance)	By following the guidelines, procedures, standards set by NIST and statues	SCADA, computers, servers, databases	Technical staff working for critical infrastructure operators	Throughout all lifecycle of the infrastructure	To make sure that all of proc
Enterprise Perspective	All of the efforts from the policy level to the tactical level	By fulfilling the requirements of the policies, procedures, and guidelines	All levels of critical infrastructures	All of the related departments, centres, institutes, groups	Before, during and after cyber incidents	For the resilient critical infrastructures that will contribute to the prosperity of the USA

7 Discussion and conclusions

This paper is the first attempt to use Enterprise Architecture for a nationwide complex enterprise, composed of many organisations of varying types and sizes. Because the CIPP of the USA is an extremely complex environment, the Zachman framework is used to conceptualise the enterprise rather than making a shadow copy. The resulting matrix was shared with two experts who were familiar with the CIPP of the USA. Both experts emphasised that Zachman's matrix is useful in demonstrating the change of the key actors with changing levels. Experts also appreciated bringing the different levels of the CIPP into the light. Therefore, the first results of the application show that the Zachman framework may be helpful for not only novice experts but also experienced ones.

As the second step of the research, the developed Zachman matrix will be elaborated on. The focus of the elaboration is to see as many responsibilities assigned in a single matrix. The matrix described in this paper can be named as a version-one matrix that gives the overview. Version-two matrix will contain more particular and actual role and responsibilities. As the second step of the future research, for each key stakeholder, a separate Zachman matrix will be created. Therefore, apart from seeing the whole CIPP program in a single matrix, the points of view of individual key stakeholders will be analysed by the help of separate matrices.

As another future study, authors also consider modelling the multi-organisational structure of CIPP of the USA by using the system of systems approach (Keating et al., 2003; Keating and Katina, 2011). The elaborated Zachman matrix can be utilised as the beginning step of this future study.

The abstractions used in creating the matrix can be regarded as a shortcoming of the representation of CIPP by using the Zachman framework. Although none of the stakeholders are excluded from the matrix, many specific roles and responsibilities are kept out, for the sake of clarity and in order not to lose the high-level point of view. Nevertheless, it is essential to represent the CIPP by using the Zachman framework to have a general view. It is also important to state that this study is the first study of its kind.

References

Andress, A. (2003) *Surviving Security: How to Integrate People, Process, and Technology*, 2nd ed., Auerbach Publications, New York.

Beltran, F. and Fontenay, A.D. (2005) 'Internet as a critical infrastructure: lessons from the backbone experience in South America', *Commun. Strateg.*, Vol. 58, No. 2, pp.1–34.

Canada (2009) *Action Plan for Critical Infrastructure*.

Carter, B., Moorthy, S. and Walters, D. (2016) 'Enterprise architecture view of complex system governance', *Int. J. Syst. Syst. Eng.*, Vol. 7, Nos. 1–3, pp.95–108 [online] https://doi.org/10.1504/IJSSE.2016.076126.

de Bruijne, M. and van Eeten, M. (2007) 'Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment', *J. Contingencies Crisis Manag.*, Vol. 15, pp.18–29 [online] https://doi.org/10.1111/j.1468-5973.2007.00501.x.

Department of Defense (2008) *Systems Engineering Guide for System of Systems*, Version 1.0.

Department of Homeland Security (2013) *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience*.

Department of Homeland Security (2016) *National Cyber Incident Response Plan*.

Dunn, M. and Wigert, I. (2004) *International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries*, ETH, Zurich.

Ekstedt, M. and Sommestad, T. (2009) 'Enterprise architecture models for cyber security analysis', *Power Systems Conference and Exposition*, IEEE, Seattle, pp.1–6.

Ertaul, L. and Sudarsanam, R. (2005) 'Security planning using Zachman framework for enterprises', in Kushchu, I. and Kuscu, M.H. (Eds.): *The First European Mobile Government Conference*, Mobile Government Consortium International LLC, Brighton, pp.153–162.

Eusgeld, I., Nan, C. and Dietz, S. (2011) ''System-of-systems' approach for interdependent critical infrastructures', *Reliab. Eng. Syst. Saf.*, Vol. 96, pp.679–686 [online] https://doi.org/10.1016/j.ress.2010.12.010.

Feltus, C., Ouedraogo, M. and Khadraoui, D. (2014) 'Towards cyber-security protection of critical infrastructures by generating security policy for SCADA systems', in Ouksel, A.M. and Nouali-Taboudjemat, N. (Eds.): *1st International Conference on Information and Communication Technologies for Disaster Management*, IEEE, Algiers, pp.1–8.

Gartner IT Glossary (2016) [online] http://www.gartner.com/it-glossary/enterprise-architecture-ea/ (accessed 5 February 2016).

Idaho National Laboratory (2006) *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, No. INL/EXT-06-11464, 911792 [online] https://doi.org/10.2172/911792.

Karabacak, B., Yildirim, S.O. and Baykal, N. (2016) 'Regulatory approaches for cyber security of critical infrastructures: the case of Turkey', *Comput. Law Secur. Rev*., Vol. 32, No. 3, pp.526–539.

Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., Peterson, W. and Rabadi, G. (2003) 'System of systems engineering', *Eng. Manag. J.*, Vol. 15, No. 3, pp.36–45.

Keating, C.B. and Katina, P.F. (2011) 'Systems of systems engineering: prospects and challenges for the emerging field', *Int. J. Syst. Syst. Eng.*, Vol. 2, Nos. 2–3, pp.234–256.

Kelly, B.B. (2012) 'Investing in a centralized cybersecurity infrastructure: why 'hacktivism' can and should influence cybersecurity reform', *Boston Univ. Law Rev.*, Vol. 92, pp.1663–1711.

Klimburg, A. (Ed.) (2012) *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn.

Kozlowski, A. (2014) 'Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan', *Eur. Sci. J.*, Special Edition, February, Vol. 3, pp.237–245.

Kröger, W. (2008) 'Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools', *Reliab. Eng. Syst. Saf.*, Vol. 93, pp.1781–1787 [online] https://doi.org/10.1016/j.ress.2008.03.005.

Little, R.G. (2003) 'Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems', *36th Annual Hawaii International Conference on System Sciences*, IEEE, Big Island, HI, USA, 9pp [online] https://doi.org/10.1109/HICSS.2003.1173880.

Oda, S.M., Fu, H. and Zhu, Y. (2009) 'Enterprise information security architecture a review of frameworks, methodology, and case studies', *2nd IEEE International Conference on Computer Science and Information Technology*, IEEE, Beijing, pp.333–337.

Orlowski, S. (2001) 'Information management: protecting critical information assets', *Comput. Law Secur. Rep.*, Vol. 17, pp.182–185 [online] https://doi.org/10.1016/S0267-3649(01)00313-2.

Pulkkinen, M., Naumenko, A. and Luostarinen, K. (2007) 'Managing information security in a business network of machinery maintenance services business – enterprise architecture as a coordination tool', *Journal of Systems and Software*, Vol. 80, No. 10, pp.1607–1620 [online] https://doi.org/10.1016/j.jss.2007.01.044.

Rinaldi, B.S.M., Peerenboom, J.P. and Kelly, T.K. (2001) 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *IEEE Control Syst. Mag.*, Vol. 21, No. 6, pp.11–25.

Rinaldi, S.M. (2004) 'Modeling and simulating critical infrastructures and their interdependencies', *37th Annual Hawaii International Conference on System Sciences (HICSS'04)*, IEEE, Big Island, pp.1–8.

Romero, D. and Vernadat, F. (2016) 'Enterprise information systems state of the art: past, present and future trends', *Comput. Ind.*, Vol. 79, pp.3–13 [online] https://doi.org/10.1016/j.compind.2016.03.001.

Rosa, J. (2008) 'Evaluating disaster recovery readiness with Zachman framework', in Mann, S. and Verhaart, M. (Eds.): *22nd Annual National Advisory Committee on Computing Qualifications*, Napier, p.178.

Sowa, J.F. and Zachman, J.A. (1992) 'Extending and formalizing the framework for information systems architecture', *IBM Syst. J.*, Vol. 31, No. 3, pp.590–616.

Tatar, U., Calik, O., Celik, M. and Karabacak, B. (2014) 'A comparative analysis of the national cyber security strategies of leading nations', in Liles, S. (Ed.): *Proceedings of the 9th International Conference on Cyber Warfare and Security*, Academic Conferences and Publishing International Limited, pp.211–218.

Tatar, U., Karabacak, B. and Gheorghe, A. (2016) 'An assessment model to improve national cyber security governance', in Zlateva, D.T. and Greiman, V.A. (Eds.): *11th International Conference on Cyber Warfare and Security*, ACPI Limited, Boston, pp.312–319.

Thacker, S., Pant, R. and Hall, J.W. (2017) 'System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures', *Reliab. Eng. Syst. Saf.*, Vol. 167, pp.30–41 [online] https://doi.org/10.1016/j.ress.2017.04.023.

The Federation of Enterprise Architecture Professional Organizations (2013) *A Common Perspective on Enterprise Architecture*, No. 9, p.4.

The White House (2013) *Presidential Policy Directive /PPD-21, Critical Infrastructure Security and Resilience*.

Tolone, W.J., Johnson, E.W., Lee, S-W., Xiang, W-N., Marsh, L., Yeager, C. and Blackwell, J. (2009) 'Enabling system of systems analysis of critical infrastructure behaviors', in Setola, R. and Geretshuber, S. (Eds.): *Critical Information Infrastructure Security*, pp.24–35, Springer Berlin Heidelberg, Berlin, Heidelberg [online] https://doi.org/10.1007/978-3-642-03552-4_3.

Urbaczewski, L. and Mrdalj, S. (2006) 'A comparison of enterprise architecture frameworks', *Issues Inf. Syst.*, Vol. 7, No. 2, pp.18–23.

Walters, D., Moorthy, S. and Carter, B. (2014) 'System of systems engineering and enterprise architecture: implications for governance of complex systems', *Int. J. Syst. Syst. Eng.*, Vol. 5, p.248 [online] https://doi.org/10.1504/IJSSE.2014.065755.

Zachman, J.A. (2003) *Excerpts from the Zachman Framework for Enterprise Architecture: Primer for Enterprise Engineering and Manufacturing*, Zachman International, Inc.

Zachman, J.A. (2009) 'John Zachman's concise definition of the Zachman framework', in Kappelman, L.A. (Ed.): *The SIM Guide to Enterprise Architecture*, pp.106–110, CRC Press, Boca Raton.