DAKOTA STATE
UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Glenn Papp Jr. Student ID: A00214253

Dissertation Title:
E-Democratic Government Success Framework for United States' Municipalities

Graduate Office Verification: DocuSigned by: Abby Chowning F44C8D9E621C417... Date: 12/07/2023

Dissertation Chair/Co-Chair: DocuSigned by: Dr. William Bendix 1B467BFB94B6418... Date: 12/07/2023
Print Name: Dr. William Bendix

Dissertation Chair/Co-Chair:_________________________ Date: ____________
Print Name: ____________________________

Committee Member: DocuSigned by: Dr. Cherie Noteboom 897E5127036A49C... Date: 12/07/2023
Print Name: Dr. Cherie Noteboom

Committee Member: DocuSigned by: E0CE171C3CDE419... Date: 12/07/2023
Print Name: Dr. Jun Liu

Committee Member: DocuSigned by: 98741E5312054CC... Date: 12/07/2023
Print Name: Dr. Petter Lovaas

Committee Member:_________________________ Date: ____________
Print Name: ____________________________

Submit Form Through Docusign Only
or to Office of Graduate Studies
Dakota State University

DAKOTA STATE UNIVERSITY

E-DEMOCRATIC GOVERNMENT SUCCESS FRAMEWORK FOR UNITED STATES' MUNICIPALITIES

A doctoral dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

October 2023

By
Glenn Papp Jr.

Dissertation Committee:
Dr. William Bendix
Dr. Wayne Pauli
Dr. Cherie Noteboom
Dr. Jun Liu
Dr. Petter Lovaas

ACKNOWLEDGMENT

First and foremost, I am extremely grateful to each of my committee members, who were instrumental in the creation of this work. To the late Dr. Wayne Pauli, although I wish we could have one last conversation, this acknowledgment will have to suffice. Words cannot express my gratitude for the time and effort that you gave me, how you saw and believed in my vision from the beginning, and how you encouraged me to overcome adversity. I am deeply indebted to Dr. William Bendix, who rescued this work, believed in my vision just as Dr. Pauli had, and closely assisted me in significantly improving the quality, scope, and organization of this research. I would like to extend my sincere thanks and recognition to Dr. Cherie Noteboom for participating in this committee and helping me grow as an academic since my enrollment at DSU. I would also like to recognize and thank Dr. Jun Liu for participating in this committee and for his expert advice on decision support systems. Last but certainly not least, I could not have undertaken this journey without Dr. Petter Lovaas, as I would have never pursued a terminal degree without his convincing arguments and encouragement. Dr. Lovaas has also worked closely with me on this research and other work—meaning he has had to put up with many hours of my rambling thoughts throughout the years. Sincerely, great thanks to each of you.

I am also grateful to the Criminal Justice faculty at Niagara University, who prepared me to pursue a terminal degree and motivated me to pursue this topic. Specifically, the courses offered by Dr. Timothy Ireland, Dr. Craig Rivera, Dr. Timothy Lauger, Dr. Paul Schupp, Professor Ron Winkley, Dr. Elizabeth Brown, and Dr. Talia Harmon exposed me to critical tools and knowledge needed for this research and led me to consider that many policing challenges could be addressed by changes to public policy and increased citizen engagement.

Special thanks to my family, especially my mother, who helped me manage my responsibilities while I was in school whenever they could. I am also grateful to Jermaine Lamarr Cole, who inspired me to address this research problem through his song, “Brackets.”

Finally, I give the most heartfelt thanks to the two people I love most: my future wife and my firstborn daughter. You both have sacrificed so much alongside me in the last few years in the pursuit of a better life for all of us. For every time I had to take an emergency phone call, a meeting ran too long, or I took an hour to “finish my thought,” we will have a hundred laughs, smiles, and memories to make in the future.

ABSTRACT

This project develops a comprehensive E-Democratic Government Success Framework that addresses low citizen engagement in local US politics. To develop this framework, I consult the literature on democratic participation, socio-technical theory, data security and privacy, decision support systems, and design science methodology. The main contribution of this project is a five-part method artifact for implementing E-Democracy initiatives—something that has not been readily attempted, despite the decentralized nature of US democracy and the opportunities it offers to experiment with institutions and deliberative procedures. This artifact gives policymakers the means to design, implement, adopt, and evaluate E-Democracy services; and it gives citizens and third parties, such as independent watchdogs, the ability to evaluate E-Democracy initiatives. Additionally, it contributes to the growing research agenda that considers the integration of information communication technology (ICT) into the policymaking process. To evaluate the effectiveness of this artifact, I use three methods: (1) benchmarking through a comparative gap analysis of the artifact's requirements, past E-Democracy initiatives in the United States, and cybersecurity frameworks; (2) scenario creation that considers the artifact's application through a synthetic lawsourcing instantiation; and (3) application of defense in depth methodology through mapping artifact requirements that overlap.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Glenn Papp (Jr)

Glenn Papp Jr.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Background of the Problem

Citizen engagement in US municipal politics is limited, even though citizens are impacted by the actions of local government to a much greater extent than those of the federal and state governments (Holbrook & Weinschenk, 2019). Both the news media and highly engaged voters focus on national politics more than they do local politics, and this misaligned focus plays a role in the persistently low participation rates in local elections (Andrews & Pruysers, 2022). In turn, low participation in local elections increases the likelihood that the "voice of the people" in municipalities becomes severely distorted—often in a biased or discriminatory way (Hajnal & Lewis, 2003). Low participation in local elections also increases the likelihood that local governments are less responsive to citizens and that their policies are less representative of citizens' preferences, especially because voters and nonvoters have consistently different views and priorities (Leighley & Nagler, 2013).

E-Government presents a possible solution to the challenges of low participation in local politics, as use of E-Government can increase citizens' trust, interactions, and perceived responsiveness with government (Tolbert & Mossberger, 2006). Opportunities for citizen participation in local politics (voting in elections and attending public meetings) are antiquated and growing scarcer by the year—especially after the onset of the COVID-19 pandemic (Salvino et al., 2012; Farris & Holman, 2023). Citizens enjoy the opportunities and conveniences provided by the Internet in the private sector and have for some time, but these advantages have yet to be incorporated to the same extent in the public sector (Tassabehji et al., 2007; Orozco, 2016). Another consequence of this service gap is its opportunity cost: not only could the use of E-Government services enable direct participation and communication, but it could also provide indirect benefits like citizen learning, decision support, and more.

Statement of the problem

This research seeks to address the problem of low citizen engagement in US municipal politics through the design and evaluation of a comprehensive E-Democratic Government Success Framework. The problem of low citizen engagement in US municipal politics is exacerbated by the lack of comprehensive literature in this area and how the deeply rooted problems of voter apathy and unresponsive government tend to continually reinforce each other (Putnam, 2001). While some relatively new democracies have successfully implemented E-Democracy platforms or initiatives, like Brazil's *E-Democracia* platform (https://edemocracia.camara.leg.br/) and Estonia's Digital Society initiative (https://e-estonia.com/), the US has yet to make meaningful strides in E-Democracy (Orozco, 2016). This gap is striking since US federalism provides many opportunities for local political experimentation and institutional innovation. Ideally, states and municipalities operate as "laboratories of democracy," but national parties have driven state and local level politics towards national concerns, effectively converting many local governments into "laboratories against democracy" (Grumbach, 2022). With that in mind, I offer E-Democracy strategies in this project that are specifically designed to enhance civic engagement in politics across the United States.

Objectives of the dissertation

This project develops a comprehensive E-Democratic Government Success Framework that addresses low citizen engagement in local US politics by defining the processes for design, implementation, use, and evaluation of E-Democratic Government services. This artifact gives policymakers the means to design, implement, adopt, and evaluate E-Democracy services; it gives citizens and third parties, such as independent watchdogs, the ability to comprehensively evaluate E-Democracy initiatives; and it provides researchers with a research agenda for E-Democratic Government. Developing E-Democracy solutions requires a multi-disciplinary approach, since the analytical tools for diagnosing the problem will differ from the analytical tools for developing and evaluating solutions. For this reason, the project will draw upon a diverse literature that covers everything from democratic engagement and sociotechnical theory to data security and design science methodology. I will consult both scholarly research and governmental reports that consider previous efforts to establish E-Democracy systems, and I will place considerable weight on research that assesses initiatives from the government-to-citizen perspective. In reviewing this diverse body of literature, I will address a series of related questions that will help me identify the strengths of and weaknesses in E-Democracy approaches, and that will help me develop targeted and effective digital solutions for US municipalities:

- What is E-Democracy and what is considered success in E-Democracy? Which related theories and research areas should E-Democracy researchers consider? How does E-Democracy differ from other related forms of governance (i.e., e-government, digital government, direct democracy, deliberative democracy, etc.)?
- What are the weaknesses of E-Democracy and deliberative democracy? What has hindered the success of E-Democracy and deliberative democratic initiatives in the past? How could E-Democracy successfully address the low levels of political awareness and interest that citizens have about local US politics?
- In developing guidance for the design, implementation, adoption, and evaluation of E-Democracy initiatives, how could that guidance: (1) address existing and emerging threats to success; (2) enshrine principles of democratic governance such as equality, inclusiveness, transparency, accountability, and responsiveness; (3) mitigate risks of failure in trust in government, design, citizen engagement, security, and privacy; and (4) increase the likelihood of success?

The terms E-Government, Digital Government, E-Governance, and E-Democracy are often used interchangeably in scholarly literature. Agawu (2017) defines E-Government as, “the delivery of government information and services online through the Internet or other digital means” (p. 3). The breadth of this definition pairs well with the ambition of this project but needs further refinement to exclude initiatives that do not increase democratic engagement. Orozco (2016) defines E-Democracy as “the digitization of decision-making processes regulated by law and increasing citizen engagement in civic and political activity through the use of technology” (p. 163). This definition aligns with what this research seeks to accomplish but excludes initiatives that do not digitize decision making processes. As my research seeks to include initiatives that do not directly digitize decision making but nonetheless contribute to furthering citizen engagement (e.g., citizen learning), I suggest a hybrid term. Borrowing from

Agawu (2017) and Orozco (2016), I define E-Democratic Government as the digital means for delivering government information and services with an aim to increase citizen engagement in civic, deliberative, and political activity.

The remainder of this dissertation is structured as follows. In the next chapter, I review the literature on E-Democracy, E-Government, deliberative democracy, decision support systems, and security research to define E-Democracy; identify which problems E-Democracy can address; and analyze past and existing E-Democracy projects for what has and has not worked and why. I then review theories in trust in government, socio-technical theory, citizen engagement, security, and privacy literature, showing how each of these areas of concern are relevant to the design of the artifact. The artifact is presented in the fourth chapter of this dissertation and is evaluated in the fifth chapter through benchmarking, scenario creation, and logical reasoning/informed argument. Finally, I conclude this work by discussing limitations and implications of this research on current and future practices and research.

CHAPTER 2

LITERATURE REVIEW

The purpose of this literature review is to explore the various strategies that E-Democracy projects offer for addressing low levels of political knowledge and engagement among citizens at the local or municipal level. Specifically, in this section, I examine the political, technical, and sociological challenges that e-strategies must overcome in order to increase civic participation. I also consider the strategies that are most likely to succeed.

Given the scope of my research, I need to consider and discuss scholarship across multiple disciplines. To begin, and to establish conceptual clarity for this project, I review how E-Democracy is different from E-Government and I examine where E-Government research can inform E-Democracy. I also consider how the research areas of deliberative democracy and E-Democracy align and where they differ. Then I review problems that E-Democracy could feasibly address in local US politics, including low participation rates in municipal elections and the unrepresentative policies that arise in low-turnout jurisdictions. After reviewing previous E-Democracy initiatives in the US, I discuss how decision-support systems that enable machine learning and text-mining techniques have the potential to spur innovation in E-Democracy initiatives. Finally, I review the roles of security and privacy in such an initiative.

E-democratic government: e-government or e-democracy?

E-Government is concerned primarily with implementing government information and services into technology, whereas E-Democracy is concerned with increasing citizen engagement, discussion, and decision making using technology. Although E-Democracy is a form of E-Government and the definitions of E-Government and E-Democracy have some similarity, the differences between the two could be as great as the dissimilarity between democratic and autocratic governance. As this research seeks to promote the principles of E-Democracy through the vehicle of E-Government methods, I briefly discuss the similarities and differences of their definitions.

E-Government, the most general of all the relevant terms, does not have a uniform definition across literature. Agawu (2017) defines E-Government as “the delivery of government information and services online through the Internet or other digital means" (p. 3). AISuwaidi & Rajan (2013) use a very similar definition: "the use of information and communication technologies (ICTs) to improve the activities of public sector organizations" (p. 161). However, Antoni et al. (2017) adopt the following definition based on the work of Gil-Garcia & Martinez-Moyano (2007): "a government way in utilizing IT to enhance transparency and trust innovatively by applying the use of web-based portal systems" (p. 1). Perceptions of transparency and trust influence individual attitudes and beliefs, which themselves have significant influence on E-Services utilization (Hossan & Ryan, 2018). As my research problem is concerned with increasing democratic engagement, the inclusion of transparency and trust considerations in this research is critical.

Conceptually, the term "E-Government" is too broad for my purposes, as this project seeks to increase citizen engagement in democratic government. E-Government considers every relationship relevant to government, including those with citizens, businesses, other governments, and public-sector employees (Agawu, 2017, p. 3). From this perspective, it is important to acknowledge that technological advancement could certainly improve each of these tenets of E-Government. However, this work is most interested in the government-to-citizen (G2C) category as the research problem is concerned with voter apathy and ignorance in local US politics. Agawu (2017) further refines this category of E-Government by proposing three trends of G2C activity: (1) increasing access to information, which is the use of digital platforms or services to facilitate citizen access to relevant content; (2) digitizing the service loop, which is the process of digitizing some element of the government service while leaving the essential function unchanged; and (3) expansion or creation of new governance function, which is the use of technology to expand or create a government service that cannot readily be said to have a non-digital parallel (p. 3).

These trends can be seen as a scale: (1) at minimum, access to content must be increased by an E-Democracy initiative; (2) it is reasonable for citizens to expect that modern initiatives digitize existing analog functions, as private sector advances in ICT correlate with citizen expectations of ICT use in the public sector (Tassabehji et al., 2007); and (3) the overarching goal of E-Democracy initiatives ought to be creating new or expanding current government functions into ones that could not be had without technology.

Although it is also conceptually broad, the term “E-Democracy” is closer to what this research seeks to accomplish in that its definitions typically focus on increasing citizen engagement. E-Democracy is defined by Grönlund (2003) as “use of IT in democratic processes” (p. 93). The author also classifies democratic decision making processes through a policymaking cycle model, starting with: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and ending with (5) monitoring the policy (p. 95). Lidén (2013) writes that the simplicity of this definition implies that the term E-Democracy is merely convenient shorthand for any IT use in democratic processes and, instead, adopts the following definition: “the use of information and communication technologies in democratic political processes concerning information, discussion and decision-making” (p. 219). Similarly, Orozco (2016) defines E-Democracy as “the digitization of decision-making processes regulated by law and increasing citizen engagement in civic and political activity through the use of technology” (p. 163). These definitions differ in semantics but seek the same result: digitizing decision making and the processes informing it to increase citizen engagement in civics and politics. For this reason, I conclude that the overarching goal of E-Democracy is to increase information, discussion, and decision making using technology.

Although these two terms have differences, there is a similarity in what is considered success in their respective research areas: creation of government functions that would not be possible without technology. To be properly regarded as E-Democracy initiatives, platforms must make digital democratic decision making possible through online technology. Concurrently, E-Government G2C trends identify the expansion or creation of new government functions that have no non-digital parallel as innovative in that field (Agawu, 2017). I notice an implicit connection between these areas, in that Agawu’s (2017) first two E-Government G2C trends—increasing access to content and digitizing the service loop— largely focus on what is generally considered E-Government activity. On the other hand, the third E-Government G2C trend—expanding or creating new government functions that have no non-digital parallel—would generally apply to any initiative that shares the same goal as E-Democracy. This is because the digitization of decision making and its foundational processes would allow for such expansion by making certain functions possible, more accurate, or more feasible where they otherwise could not be without technology (e.g., real-time data analysis at different stages of decision making, digital citizen learning requiring fewer human resources, etc.).

Because current terms in the literature are either too broad or too narrow for my purposes, I propose a new term: E-Democratic Government. Borrowing from Agawu (2017) and Orozco (2016), I define E-Democratic Government as the digital means for delivering government information and services with an aim to increase citizen engagement in civic, deliberative, and political activity. In other words, it is the formal effort to enhance democracy through the use of online technology. While E-Government literature puts focus on integrating technologies into government regardless of use, E-Democracy literature has more of a focus on the integration of technology into democratic processes—which indirectly can increase citizen engagement. Although the difference is small, use of E-Democratic Government explicitly requires seeking to increase citizen engagement.

E-democracy and deliberative democracy

There is already an extensive E-Democratic infrastructure in place, but it is being used not with any specific normative purpose in mind, but rather with an aim to give existing influential political actors even greater influence in shaping political and policy outcomes. Private actors, from American political parties to lobbyists and special interest groups, exploit partisan systems (e.g., direct communication from campaigns to citizens through emails and web services), competitive-elitest networks (e.g., opinion polling through SMS texting), and knowledge sharing platforms (e.g., Wikis) for their own interests—driving polarization and misinformation while undermining deliberative participation (Alathur et al., 2011). The private sector already uses community-based systems, but so far, the public sector has not adopted them. The American public sector has dabbled with monitorial networks—through which citizens express nonemergency grievances and dissatisfactions, often directed at elected officials, to pave the way to change systems (Alathur et al., 2011, p. 12)—but has not attempted to start any other type of E-Democracy forum (Orozco, 2016). Political parties appear to have no difficulty organizing activities using email, web sites, and other digital means, but the deliberative and monitorial aspects of American E-Democracy—especially in municipalities—are much more primitive, if they exist at all.

E-Democracy can provide a means for fostering constructive citizen participation in politics when it shares the normative ambitions of the deliberative democracy literature. In offering a broad summary on deliberative scholarship, Bächtiger et al. (2018) define deliberation as “mutual communication that involves weighing and reflecting on preferences, values, and interests regarding matters of common concern,” and they define deliberative democracy as “any practice of democracy that gives deliberation a central place” (p. 2). The authors contrast deliberative democracy from aggregative democracy in that the latter is concerned only with counting votes and identifying majorities, whereas deliberative democracy is concerned with helping citizens better understand where they and others stand on issues, fostering agreement where possible, and clarifying or structing conflicts that will go up for a vote. Further, Bächtiger et al. (2018) identify several standards for “good deliberation,” including the ideals of mutual respect, absence of coercive power, equality, reason, consensus, orientation to the common good, publicity, accountability, and sincerity.

Importantly, key standards for good deliberation, including absence of coercive power, accountability, and equality, are potentially achievable through the administration of a digital system. For example, Hansson et al. (2014) have developed software for group collaboration that generates, reports, and updates in real time a participation score for each user in order to reveal any power imbalances. In doing so, this software helps further to fulfill several deliberative ideals: (1) participants are equal members, (2) participants set the agenda together, (3) participants can fully participate in the discussion, (4) all participants have the same status when decisions are taken, and (5) everyone has an informed understanding of the discussion. Indeed, these ideals share the same principles as the criteria for good deliberation established by Polletta and Gardner (2018), among many other deliberative democracy scholars (p. 71).

Hansson et al. (2014) briefly discuss how digital deliberative systems can provide autonomy that goes beyond autonomy offered by conventional deliberation—often exploited by private actors or centralized states for their own interests. This is possible due to the reputational value systems that allow for the community to link to, like, blog about, dig, and/or tweet validating content. eBay is given as an example of this distinction, in that reputation and quality of sellers comes from a decentralized customer validation of trustworthiness through ratings rather than eBay or the seller assigning such a rating. In reputational value systems, the network is the organizational principle instead of some centralized entity (Hansson et al., 2014, p. 158). Although many principles of deliberative democracy are enforceable using technical controls, principles that cannot be enforced this way (i.e., mutual respect, reason, orientation to the common good, and sincerity) must be enforced through policy and moderation.

Effect of declining social capital on democracy

Because E-Democracy aims to increase citizen engagement, discussion, and decision making using technology, it promises an effective means for addressing low engagement in local US politics. But to be frank, the challenges of low engagement are enormous. As the political science literature shows, voter apathy and unresponsive government policy are deeply rooted problems that continually reinforce each other. Citizens feel increasingly alienated; they participate less in politics; governments ignore the needs of nonvoters; citizens grow more pessimistic and alienated; and so on.

In the past half century, communities have frayed and, consequently, voter participation has declined in municipal elections. Putnam (2001) argues that social capital, that is, relationships of trust and reciprocity among citizens, is crucial for maintaining robust, effective democracies. But as Putnam shows, social capital—along with its main drivers, civic engagement and group membership—has declined sharply in communities across the United States since the mid-twentieth century. The main reasons for this decline in order from most to least impactful, according to Putnam (2001), are generational change, the effect of electronic entertainment, suburbanization/commuting/sprawl, and pressures of time and money (p. 289). Putnam (2001) reasons that the latter two reasons could not account for more than 20% of declining social capital, and it is reasonable to assume that this is still the case today. However, the first two reasons—especially electronic entertainment—have grown more relevant thanks to the COVID-19 pandemic and the permeation of technology into daily life.[1]

Studies on municipal politics reinforce Putnam's appraisal. Indeed, several studies estimate that, at best, one-quarter of eligible voters participate in local elections (Alford & Lee, 1968; Morlan, 1984; Bridges, 1997). The result, as Hajnal & Lewis (2003) explain, is that "at the local level where policies are most likely to be implemented and where a majority of the nation's civic leaders are being elected, important public policy decisions are being made without the input of most of the affected residents" (p. 646). In other words, powerful interests

[1] A dangerous consequence of this shift is how the same information can be delivered with different narratives. For example, in a nationwide, online survey of 520 US adults regarding views of police and local government, those with more exposure to frequent terrorism print news had lower opinions of police, but those with more exposure to frequent national television news had higher opinions of police (Banjak-Corle & Wallace, 2020). Separately, consumption of private online content for entertainment is much easier and more convenient than socializing publicly or joining community groups.

and the most engaged voters end up receiving the municipal government's full attention, while the most marginalized residents are neglected and further marginalized. Predictably, decades of data show that the income gap between voters and nonvoters is staggering (Leighley & Nagler, 2013). Kersting (2012) also acknowledges the political divide of have and have-nots and writes that digital democracy must prevent the conversion of political have-nots to digital have-nots. Hajnal & Lewis (2003) review several institutional remedies and their impacts on municipal election turnout using surveys mailed to California municipal city clerks in late 2000. They find that two reforms are effective in encouraging nonvoters to become voters: holding municipal elections on the same days as larger elections and offering ballot initiatives on major local services (such as policing, water treatment, and garbage removal; see also Zheng et al., 2014; Kouba et al., 2021). Of course, as Hajnal & Lewis (2003) caution, higher turnout does not necessarily lead to higher levels of civic engagement, especially over the medium and long term. If residents have no ongoing incentive or opportunity to learn about local political developments, participation rates quickly drop.

Ultimately, persistently low turnout and institutionalized marginalization leads to the erosion of democratic practices. In fact, democratic backsliding at the state and local levels has intensified in recent years across the US. Part of the problem is the cycle of apathy and unresponsiveness discussed above. But another factor is that the political parties, increasingly gridlocked at the national level, seek to control policy elsewhere, namely, at the state and local levels. The Republican Party, more so than the Democratic Party, has sought one-party rule in local jurisdictions to lock-in ideologically extreme policies that satisfy their donors and most loyal partisan voters at the expense of the majority. In effect, Republicans have turned states and, where possible, municipalities into "laboratories against democracy" (Grumbach, 2022). Even when local elected officials are not tied directly to a national party, they will often take policy actions that reflect their preferred party's interests—sometimes at the expense of their community's well-being. For example, Farris & Holman (2023) show that rightwing sheriffs often refused to enforce mask mandates during the height of the COVID-19 pandemic.

The state of e-democracy in the US

There is a notable gap between the capabilities of past US E-Democracy initiatives and those of some other countries. Brazil and Estonia, for example, have successfully implemented

E-Democracy initiatives that fit within the scope of the E-Government G2C trends in that they (1) increase access to content, (2) digitize the service loop, and/or (3) expand or create new government functions (Agawu, 2017; Orozco, 2016). Brazil's *E-Democracia* platform allows users to review, rate, and propose edits to existing law and proposed legislation (Orozco, 2018). Estonia's Digital Society initiative provides citizens digital access to identity services, cybersecurity information, interoperability services, healthcare services, e-Governance services, smart city and mobility services, tax and financial services, and education or research. These initiatives have features that provide access to content, digitize the service loop, and expand or create government functions that do not have a non-digital parallel.

The list of past and current E-Democracy initiatives in the US is astonishingly small. In the federal government, the first digital service offered that went beyond access to government information was a monitorial platform called *We The People*, launched by the Obama administration in 2011 (Orozco, 2016). If a petition, which could be submitted by any US citizen, obtained more than 100,000 signatures, presidential review and a response were guaranteed by the administration within 30 days. Although perceived responsivity increased thanks to this platform, some "entertaining" but purposeless petitions attracted public support, e.g., one that sought to build the *Star Wars* Death Star by 2016 (Orozco, 2016, p. 163). The only other E-Democracy initiatives in the federal government since then have been self-serving: one to crowdsource an art review instead of using taxpayer dollars by the US Patent and Trademark Office in 2012, and one to crowdsource a strategic innovation policy report for the White House Office of Science and Technology in 2014 (Orozco, 2016).

State and local governments, on the other hand, have more E-Democracy history to offer than does the federal government (although, not by much). In 2009, the Mayor's Office in Boston, Massachusetts, unveiled a new platform called *Citizens Connect* (now called *Boston311*; Agawu, 2017). *Boston311* digitizes the service loop by enabling citizens to report potholes, broken traffic lights, and other issues directly to the government, and then allowing them to track responses to those issues. Admittedly, similar attempts to digitize the service loop at the state or local levels exist throughout the US (e.g., NYC 311) but are not included for brevity. In 2013, an interesting blip of E-Democracy innovation spurred in California: State Congressman Mike Gatto used *Wikispaces*, a now-defunct collaboration website, to allow his constituents to edit and make proposed changes to draft legislation (Orozco, 2016). However, Gallo chose probate law as the starting category, which only yielded a bill that would allow courts to assign a guardian to a deceased person's pet. The bill was passed by the California Assembly and Senate, but ultimately vetoed by the California Governor, and this approach has not been used there since (Heaton, 2015).

The state of E-Democracy in the US may appear weak, but the conditions for establishing robust digital services exist in many municipal jurisdictions where traditions of deliberative democracy still thrive. Indeed, because of their deliberative and broadly inclusive political practices, these jurisdictions have the potential to successfully implement E-Democratic Government to demonstrate its effectiveness and value. New England states, with their long history of townhall meetings and other direct democracy practices, stand out as especially viable locations, even though, to date, *Boston311* is the only major E-democracy initiative that has been attempted in that region (Orozco, 2016). Salvino et al. (2012) use New England states to study the connection between direct and representative democracy using town hall meetings, and astonishingly find no difference between the impact of the two, indicating again that direct democracy efforts alone are insufficient to address declining civic engagement. With the ability of systemization to establish technological boundaries to ensure good standards of deliberation, thoughtful moderation through policy to sure up the standards that cannot be achieved this way, and an institutional appetite for more direct democracy, E-Democracy could be an effective tool for reversing the decline in civic engagement across American municipalities.

Decision support systems

Often in E-Democracy, just as in democracy itself, a major challenge is to develop processes that ensure majority preferences are reflected in enacted policies. However, even determining what the majority prefers can pose a big data problem if that data comes from unstructured and decentralized sources, like social media posts. For example, Chugunov et al. (2016) discuss how the split of citizens' sentiments among *Change.org*, a news story's comment page, and a Russian television channel diluted opposition to a Russian decree banning Western imported foodstuffs (p. 44). Decision support systems (DSS) that are used in E-Government projects offer strategies for enhancing democratic responsiveness and engagement through techniques like machine learning and text mining. Sprague & Carlson (1982) define

DSS as interactive computer-based systems to help decision makers use data and models to solve unstructured problems (where structured means having processes in place to handle situations as they arise). Similarly, Shim et al. (2002) define DSS as "computer technology solutions that can be used to support complex decision making and problem solving" (p. 111). In this section, I consider how implementing decision support systems into an E-Democracy platform could enhance democratic responsiveness and engagement.

There are many considerations that affect the decision making process, such as the number and management of decision makers and the structure of the decision making process. Information technology can be applied to the decision making process but the technologies' support (or harm) to the decision making process is dependent on the technologies' development, design, and implementation. Without proper guardrails, decision making agendas and decisions themselves could be overtaken by individuals or small groups instead of being collectively determined by a majority of stakeholders. Another consequence of insufficient decision support is explained by Hahanov et al. (2016), who argue that voters elect mediocre and unworthy leaders without decision support or proper education. As an example of a system with proper guardrails, Carvalho et al. (2009) develop a Large-Scale decision support system using the Collaboration Engineering approach to decision making, which calls for task diagnosis, task assessment, activity decomposition, ThinkLet match, design documentation, and design validation. Requirements are determined in the task diagnosis stage, and the basic process is determined in the task assessment stage. The basic process is expanded upon during activity decomposition, where concepts are generated, reduced to those worthy of attention, clarified by increasing shared understanding of words and phrases, organized by relationships to other concepts, evaluated by considering relative value of the considered concepts, and finally agreed upon via a group commitment to a proposal. In the ThinkLet match stage, a ThinkLet, or "a codified facilitation technique that creates a predictable pattern of organization" (Carvalho et al., 2009, p. 52-53), is developed or chosen for the adopted proposal. The entire process is documented and modeled in the design documentation phase, and the process is pilot tested and final improvements are made in the design validation phase. A design framework like Collaboration Engineering should always inform the design of decision support systems, as such a structure in system design can greatly harden some of the standards of good deliberation identified by Bächtiger et al. (2018), such as absence of coercive power and equality among participants.

An important aspect of digitizing democratic government is the voluminous data that can be collected, stored, shared, analyzed, and used to assist decision making. However, as is often the case with digital information, decision support systems can obscure knowledge and hinder its usefulness if knowledge is not properly managed. In the literature, knowledge management is defined as "the process by which organizations leverage and extract value from their intellectual or knowledge assets" (Kulkarni et al., 2006, p. 310). Kulkarni et al. (2006) develop a knowledge management success model whereby knowledge use is hypothesized to be dependent on measures of organizational support (leadership, incentive, coworker, supervisor), measures of knowledge content quality and knowledge management system quality, and measures of perceived usefulness of knowledge sharing and user satisfaction. Although the model in Kulkarni et al. (2006) only considers explicit knowledge, Nemati et al. (2002) propose an extension to the data warehousing model, through which an infrastructure enables businesses to extract, cleanse, and store vast amounts of data, to facilitate capturing implicit knowledge that only exists in the minds of employees. The authors call the extension the knowledge warehouse model, intended for supporting decision support systems, within which organizational decision makers are provided with an intelligent analysis platform that enhances the capturing and coding of knowledge by powering the retrieval and sharing of knowledge (p. 156).

Big data analyses of traceable public activities can reveal important insights about public opinion. For example, Calderon et al. (2017) use machine learning, a technique made possible by algorithms that allow systems to learn and interactively change based on end-users' use of the system, to analyze citizen sentiment in Twitter posts' text during the 2014 Brazilian World Cup using a combination of social media analytics and a literature review of social protest and citizen trust research. In doing so, the authors conclude that protests during that time were caused by a very diverse set of grievances (p. 1686). Had the Brazilian Government known these grievances in real-time, they could have used these findings to help inform their decisions. Further, this is not a singular instance. Mossberger et al. (2013) examine the use of social networks in the 75 largest U.S. city governments between 2009 and 2011 and find that usage of Facebook and Twitter increased from 13% and 25%, respectively, to 87%. The authors also conducted case studies of Seattle, Louisville, and Chicago city governments' use of social networks during this period and found that government-to-citizen one-way push strategies dominated use, while more deliberative strategies were much less common.

Due to the increasing prevalence and use of social media, government's use, analysis, and development of social media applications and data are critical to understanding citizen trust. Many similar publications analyzing Twitter users' posts and account characteristics (location, language, number of followers) for user sentiments exist; Jaidka and Ahmed (2015) study the 2014 Indian General Election using manual content analysis, Jamal et al. (2015) study Anti-Americanism and Anti-Interventionism using machine learning, and Papp et al. (2020) study trust in government using machine learning. Although analyzing social media and similar applications is important, government officials' participation in design and use of these kinds of applications is just as critical. Starke et al. (2020) survey 1,117 German respondents on trust in government, interactions with politicians on social networking sites, and evaluations of politicians, and find that interacting with politicians on social networking sites positively affects trust in government. Further, the authors find that the only significant connection between trust in government and interactions with politicians on social networking sites is the citizens' evaluation of likeability—not leadership, responsiveness, or benevolence alone (Starke et al., 2020, p. 6). Regarding development of social media applications, Katakis et al. (2014) use DSS to offer a social voting advice application for the 2012 Greek national election. This app not only helped voters identify the party and candidates most aligned with their preferences; it also helped them monitor campaign developments and update their views, by "recording the sentiment of the electorate on issues and candidates" (p. 1039). The authors conclude that any community-based approach using decision support systems is likely to be more accurate than simple alignment with one's party, and the authors provide several usable algorithms denoting exactly how the data was processed.

Text mining, which uses machine learning to automatically summarize lengthy text for users, is a feature of DSS that highlights its potential value in fostering e-democratic participation. Charalabidis et al. (2019) describe multiple use cases of legal text mining after conducting semi-structured interviews that demonstrate the breadth of the effectiveness of DSS in different scenarios, spanning from a private individual to a parliamentary administrator. They find that users tend to prioritize tools that would impact their day-to-day lives while finding features like visualization non-essential (p. 372-373). Marques et al. (2019) propose a ranking method for finding the most salient law articles relevant to a particular motion using machine learning embedded into a search engine. Finally, Tesfay et al. (2018) propose a PrivacyGuide tool that accepts URLs leading to companies' privacy policies and provide letter grades on eleven different privacy aspects (data collection, protection of children, third-party sharing, data security, data retention, data aggregation, control of data, privacy settings, account deletion, privacy breach notification, and policy changes) using the open-source machine learning tool, WEKA (p. 19). A usable example that highlights the benefit of text mining is the *Terms of Service Didn't Read* (https://tosdr.org/) platform, which offers summaries of lengthy terms of service documentation from numerous web services and provides a letter grade based on fairness of their terms for their users.

To date, no scholarly work has considered the appropriate modeling choices or theoretical approaches for using DSS as part of an E-Democracy effort to increase the policy responsiveness of governments and the civic engagement of community members. But work on DSS and electronic voting offers some relevant insights and guidelines for developing workable E-Democracy strategies. Robertson (2005) argues that, because voting is a lengthy learning and decision making process, E-Democracy efforts need to be designed as "voter support systems" that make it easier for citizens not only to vote, but also to gather and assess relevant political information so that they can select candidates who best serve their interests (p. 270). Robertson (2005) also lists seven requirements of voter DSS: (1) integration of tasks; (2) customization and personalization; (3) information gathering; (4) information retrieval and use; (5) information sharing; (6) trust, control, and information sources; and (7) diversity of users (p. 271-4). Although this research does not focus on voting electronically, the context of voting model in Robertson (2005) is like the Agawu (2017) G2C E-Democracy trends in that the first level, vote, is more of the core, basic function. As the next levels are considered, they increasingly move past basic participation and towards the creation of a nondigital equivalent, i.e., decision making, information offering, and culture and beliefs.

Security and privacy

E-Government projects not only need to enhance democratic responsiveness and engagement, but they also need to guarantee the privacy of users and ensure digital systems are reliable and secure. We have decades of research exploring this concern. As a starting point, Bell & La Padula (1976) provide the MULTICS model, which depicts a secure computing architecture by integrating hardware, kernel, operating system, and applications together tightly. But this model has long been abandoned because developments in commercial computing, which uses hardware, kernel, operating system, and applications together *without* secure integration, became feasible and marketable—effectively setting the stage for the cybersecurity landscape we have today. More recently, Cassini et al. (2008) compare information security and privacy-related laws and regulations in both the US and the European Union and find that laws like the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach Bliley Act (GLBA) of 1999, and the Sarbanes-Oxley Act (SOX) of 2002, illustrate an intent to address information security and privacy. However, the authors find that US laws are much more piecemeal and incomprehensive as compared to European Union Directives at the time (i.e., 2002/58/EC right to privacy).

Those tasked with ensuring the computer security and user privacy of an E-Democratic Government initiative must follow cybersecurity frameworks over mere legal compliance (mostly because of how far behind US laws and regulations are comparatively). Gerber & von Somms (2008) propose a model for determining organizations' legal requirements, and in doing so, demonstrate how inadequate the laws and regulations are when compared to a comprehensive security framework like ISO/IEC 27002 or the NIST Special Publication (SP) 800 series. The US White House identifies cybersecurity as part of a wider strategy to defend critical infrastructure and, acknowledging the threats technology can pose to democracy, call for new performance-based regulations that use existing cybersecurity frameworks, voluntary consensus standards, and guidance—*not* existing laws and regulations (The White House, 2023). Further, The White House (2023) writes that "individuals, small businesses, state and local governments, and infrastructure operators have limited resources and competing priorities, yet these actors' choices can have a significant impact on our national cybersecurity" (p. 4). Accordingly, although some municipalities may lack sufficient resources, those responsible for their cybersecurity ought to secure municipal systems with the same level of protection that would be applied to critical infrastructure where possible.

Each relevant cybersecurity standard and process must be used in the correct context, and using each of these publications reinforces the effectiveness of using others per the Defense in Depth strategy. The Defense in Depth strategy developed by the NSA (US National Security Agency, 2015) is a method that calls for a balanced focus between people, technology, and operations, wherein: (1) information assurance is achieved by clear delineation of responsibility and accountability; (2) technological defense in both multiple places and layered when possible; and (3) thorough operational security via explicitly documented policy and procedures (p. 2-4). Defense in Depth has been used to further secure other niche uses of ICT: some examples include Groat et al. (2012) implementing Defense in Depth within network security by combining symmetric and dynamic defenses, as well as Mell et al. (2016) and US Department of Homeland Security (2015) implementing Defense in Depth within industrial control systems. When done correctly, layering relevant cybersecurity standards and processes provides a much more comprehensive approach to cyber defense than using only one such framework or process.

There are various frameworks, guidelines, and standards for cybersecurity, and it is unclear to the average user how to properly use these and in what context. As this research considers local US politics, I will focus on organizing cybersecurity activities around reputable cybersecurity publications by US Government agencies, such as the National Institute of Standards and Technology (NIST) under the US Department of Commerce and the National Security Agency (NSA) under the US Department of Defense (DoD). Accordingly, the NIST Cybersecurity Framework (Barrett, 2018) and the NIST National Initiative for Cybersecurity Education (NICE) Framework (Petersen et al., 2020) are the widely recommended working documents for organizational cybersecurity. The NIST Cybersecurity Framework—a set of cybersecurity activities, outcomes, and informative references separated into five categories: identify, protect, detect, respond, and recover—is better suited as an evaluation tool for cybersecurity maturity rather than a how-to guide for cybersecurity (Barrett, 2018; Miron & Muita, 2014). The NIST NICE Framework, also known as NIST SP 800-181, is a guide for creating cybersecurity workforce frameworks and helps the user to envision what tasks, knowledge, and skills would be required for new organizational roles (Petersen et al., 2020). Both are beneficial to cybersecurity, but only at certain phases of the process.

Risk management is one of the most crucial aspects to cybersecurity. NIST Joint Task Force (2018) defines risk management as "the ongoing process of identifying, assessing, and responding to risk" (p. 4). NIST SP 800-37 is a risk management framework that functions as a system life cycle for security and privacy risk assessments (NIST Joint Task Force, 2018).

NIST SP 800-37 denotes a risk management process consisting of seven steps: prepare, categorize, select, implement, assess, authorize, and monitor (NIST Joint Task Force, 2018, p. 23-83). Another commonly used theoretical model for risk management is the McCumber Cube, which assesses risk across three intersecting planes: one consisting of confidentiality, integrity, and availability; the second consisting of people, process, and technology; and the third consisting of data at rest, data in processing, and data in transit (McCumber, 2004). These must be used in tandem to foresee emerging threats as early as possible and further tailor the risk management process for E-Democratic Government.

Table 2.1. NIST SP 800-53 security and privacy control families, adopted from NIST Joint Task Force (2020), p. 8.

ID	FAMILY	ID	FAMILY
AC	Access Control	**PE**	Physical and Environmental Protection
AT	Awareness and Training	**PL**	Planning
AU	Audit and Accountability	**PM**	Program Management
CA	Assessment, Authorization, and Monitoring	**PS**	Personnel Security
CM	Configuration Management	**PT**	PII (Personally Identifiable Information) Processing and Transparency
CP	Contingency Planning	**RA**	Risk Assessment
IA	Identification and Authentication	**SA**	System and Services Acquisition
IR	Incident Response	**SC**	System and Communications Protection
MA	Maintenance	**SI**	System and Information Integrity
MP	Media Protection	**SR**	Supply Chain Risk Management

For practical guidance, NIST SP 800-53 specifies hundreds of controls for security and privacy of federal information systems separated into categories called families, listed in Table 2.1. NIST Joint Task Force (2020) defines controls as “descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders” (p. 8). Accordingly, each of these publications must be used together in administering a comprehensive risk management program. Mulligan and Schneider (2011) advocate for challenging the status quo of cybersecurity’s doctrines of risk management and deterrence through accountability and they propose a doctrine of public cybersecurity, defined as “any cybersecurity doctrine whose goals are (i) to produce cybersecurity and (ii) to manage insecurity that remains, where political agreement balances individual rights and public welfare" (p. 77). Obvious gaps exist if E-Democracy Government initiatives are posited against any of these cybersecurity publications alone, as they do not consider trust in government, citizen engagement, disinformation prevention, or reputational factors (McCumber, 2004; Barrett, 2018).

Although adherence to cybersecurity frameworks is critical, a comprehensive cybersecurity program must also consider and anticipate emerging threats. The spread of disinformation is one such threat that appears directly relevant to E-Democratic Government, as the Russian Internet Research Agency successfully spread disinformation targeted at US social media users in 2016 with the purpose of stirring controversy, disagreement, and division among likely US voters (Farrell & Schneier, 2018). The US government was wholly unprepared for foreign election interference and disinformation campaigns (Prier, 2017). Reflecting on the dangers of foreign interference efforts, Farrell and Schneier (2018) suggest that we should view democracies as information systems through the lens of common versus contested knowledge, whereby common knowledge is what needs to be shared for the political system to function, and contested knowledge is material over which people may disagree (p. 6). Critically, the authors note that, if basic political or institutional facts (such as election results and succession procedures) in a society fall from common knowledge to contested knowledge, the system can no longer function (p. 8-9). For these reasons, special focus should be given to social engineering in E-Democratic Government initiatives due to the nature of collected data and how its analyses inform decision making. For example, Fu et al. (2018) discuss how to combat spammers—or users that send unsolicited messages and create unsolicited social relationships through fake accounts, social bots, or spam applications—on social networks. The authors propose a dynamic metric measuring change in user activity that also quantifies users' evolution patterns which, when combined with supervised and unsupervised machine learning, has the capability of distinguishing between legitimate and illegitimate users.

Any E-Democratic Government platform must recognize that, while most users have an interest in maintaining their privacy, they tend to have a poor track record in doing so. One problem for users is that privacy—a notoriously difficult concept to define—can pertain to physical seclusion, informational secrecy, and informational control depending on the context. Users are not necessarily making these distinctions or keeping them constantly in mind. Smith et al. (2011) specifies that information privacy, and not physical privacy, is within the scope of what most cyber or information systems research today would call privacy in this realm. The authors then further categorize what privacy is: (1) a value-based right, (2) a value-based commodity, (3) a cognate-based state, and (4) a cognate-based control—and what it is not: (1) anonymity, (2) secrecy, (3) confidentiality, (4) security, and (5) ethics (Smith et al., 2011, p. 994-7). Although the authors clarify that the value-based definitions should not be treated absolutely, as they often conflict with legal and societal frameworks, they also specify that privacy has a contextual nature. Separately, Gerber et al. (2018) discuss the privacy paradox: a privacy phenomenon where users often indicate one privacy preference when surveyed yet behave in ways that contradict their survey answers. It remains unclear what drives this paradox, but Gerber et al. (2018) suggest that the privacy paradox likely reflects a combination of cognitive biases that push users to underestimate costs from privacy losses, especially over the long term. Specifically, the authors identify four categories of predictor variables for future studies: (1) privacy attitude, concerns, and perceived risk; (2) privacy related behavioral intention and willingness; (3) information disclosure behavior; and (4) protection behavior and privacy settings (p. 249-251). Accordingly, developers need to make privacy safeguards easy to use and understand—perhaps by setting strong privacy settings as default.

Key takeaways

Having reviewed diverse literatures on E-Democracy, civic engagement, deliberative democracy, digital security, and privacy, among others, several key points are worth emphasizing. First, there is a considerable need and opportunity to establish E-Democratic Government initiatives for US municipalities. Decades of voter apathy and alienation, driven by a range of sociological factors, have created political environments in which local governments often serve the priorities of highly engaged voters and organized interests at the expense of nonvoters. As I argue, E-Democracy platforms may provide a user-friendly means to inform nonvoters of the policy issues at stake and the mechanisms for direct political engagement. Second, decision-support systems that enable machine learning and text-mining techniques have the potential to spur innovation in E-Democracy initiatives. In short, existing technologies can be used to develop online platforms for broad participatory and deliberative activities. However, any E-Democracy initiative must not only follow cybersecurity standards and processes (which often exceed current requirements in law and regulations) but must also go further by using the Defense in Depth strategy to better anticipate emerging threats and to help specialize these frameworks towards E-Democratic Government. Finally, privacy findings are complicated and unclear in the literature, so those who are tasked with ensuring user privacy in E-Democratic platforms must ensure privacy safeguards are easy to use and understand, as well as being strong by default.

CHAPTER 3

SYSTEM DESIGN (RESEARCH METHODOLOGY)

This chapter is divided into two sections. In the section on theory and artifact design, I review literature specific to building an artifact that achieves the outcomes this research desires—increased quantity and quality of civic engagement in local US politics—through trust, engagement, collaborative design, security, and privacy. In the section on implementation and validation methods, I classify this research among other renowned information systems and design science research publications. I also discuss other methodologies and choices within design science research and justify the research strategies that I adopt for this project.

Theory and artifact design

To address the multi-decade decline in local political engagement, I develop an artifact with two objectives in mind: first, to increase citizen knowledge of municipal politics and policy issues and, second, to create online opportunities for citizens to act upon their increased awareness and thereby push for responsive government action. The design of the framework artifact is guided by five related theories and/or research areas: trust in government, citizen engagement, socio-technical theory, computer security, and user privacy. In what follows, I discuss the importance of each of these for designing the artifact and I explain the methodological approaches for developing the artifact itself. Additionally, I discuss the use of lawsourcing as a strategy for evaluating the artifact and its effectiveness in increasing local citizen engagement.

In designing an artifact, it is important to recognize that trust in government as a goal represents a moving target, because citizens evaluate the credibility and reliability of government along three interconnected dimensions. Failure in one dimension will often erode trust in government as a whole. First, citizens consider the trustworthiness of public officials and whether their conduct obviously diverges from broad ethical, legal, or democratic standards. Second, citizens consider whether government services are generally dependable and effective or whether they fall short of reasonable expectations. Third, they consider whether government policies address public needs and to what extent government actions reflect (or fail to achieve) the main priorities of the community (Thomas, 1998; Tassabehji et al., 2007). Therefore, to increase civic and political engagement, E-Democratic Government initiatives need to recognize that citizens will often have low trust in government for multiple, persisting reasons and that efforts to increase trust may face serious hurdles. Importantly, such initiatives also need to make sure that they do not contribute to a further erosion in government trust. Thomas (1998) reviews the three conceptions of trust—fiduciary trust, mutual trust, and social trust—and connects them to the production of trust. Tassabehji et al. (2007) furthers this effort and defines modes of trust production in the development of a trust verification agent artifact used to generate citizen trust in adopting E-Government platforms. These modes of trust production are: (1) characteristic-based trust, tied to personal characteristics that are difficult or impossible to change; (2) process-based trust, tied to reciprocity with exchanges of equal intrinsic or economic value; and (3) institutional-based trust, which can be achieved either by individuals or the organization entirely, and/or administration of laws, regulations, insurance, and other practices (Tassabehji et al., 2007; Thomas, 1998). The best e-democratic strategy for boosting trust, and thus engagement, is to focus on continually improving each of these modes of trust production—and being transparent and honest with the target jurisdiction about those efforts (Thomas, 1998; Tolbert & Mossberger, 2006; Tassabehji et al., 2007; Aladwani & Dwivedi, 2018; Papp et al., 2020). Further, trust in technology cannot be used as a substitute for, or a shortcut to developing, trust in government. For example, Teo et al. (2008) survey 214 Singapore E-Government website users and find that trust in government—not trust in technology—is positively related to trust in E-Government websites.

Trust in government and citizen engagement are obviously linked, but artifact design needs to treat engagement as a distinct normative concern and design challenge. This is because citizens must not only trust the government but also the E-Democratic Government platform that is designed to increase participation and encourage shared decision making between citizens and public officials. Citizen engagement is defined as "the active participation of citizens, in partnership with government, in decision and policy making processes" (Olphert & Damodaran, 2007, p. 494). Batlle-Montserrat et al. (2014) identify citizens' engagement as one of the most important services provided by public administrations, and the authors describe citizens' engagement as including: (1) the satisfaction of citizens' expectations; (2) the attraction of citizens' attention; (3) the consolidation of bonds between citizens and government; (4) the encouragement of the relationship between citizens and their administrations; and (5) the promotion of or participation in E-Democracy activities by both parties (p. 62). Research has found that individual attitudes and beliefs have a significant influence on E-Services utilization (Hossan & Ryan, 2018). Relatedly, E-Services must be designed for equal accessibility and operability to be perceived as legitimately seeking more engagement (Bonacin et al., 2009; Hansson et al., 2013). Models concerning user interfaces and user experience, like the Technology Acceptance Model—consisting of the theories of Perceived Usefulness and Perceived Ease of Use—must also be applied and incorporated into design to help attain optimal engagement (Davis, 1989).

Furthermore, designers need to adopt a broad understanding of citizen engagement that encompasses more than just the public's use of the E-government platform if they want to maximize the likelihood of developing a successful service or initiative. Scholars argue that citizens should be involved in, or at least consulted during, the design process, and that their level of engagement from the early design stages to the implementation phase should be used to evaluate the effectiveness of an online platform from the standpoint of user commitment (Olphert & Damodaran, 2007; Bateman et al., 2011). For example, Bateman et al. (2011) find that the success of online discussion communities depends on "participants' willingness to invest their time and attention in the absence of formal role and control structures" (p. 841). But it is not enough to simply generate interest among potential users. As Olphert & Damodaran (2007) argue, E-government services will only meet basic benchmarks of success if the public sees the services as broadly beneficial, widely accessible, and very easy to use. Thus, the artifact proposed in this project will be guided by broad concerns of citizen engagement and usability.

Citizen engagement, moreover, must encompass inclusivity. This point may seem self-evident or redundant, but it is not. A critical step in fostering both trust in government and trust in E-Democratic Government is to include all stakeholders, and not just those with the resources to participate, in the development and implementation stages of a platform. The literature on socio-technical systems design (STSD) explains that this immersive inclusion allows for the consideration of societal aspects not commonly considered with technical design. STSD is defined as "an approach to design that considers human, social and organizational systems" (Baxter & Sommerville, 2011). Other definitions in literature appear to be sympathetic towards this definition with minor deviations (Ayyad, 2017; Cherns, 1976; Cherns, 1987; Clegg, 2000; Lyytinen & Newman, 2008; Hapsara, 2016). Specifically, Cherns (1987) gives a revised list of STSD principles that are summarized in Table 3.1. Although most principles require implementing underlying technologies correctly, technical knowledge is not required to participate in STSD as all principles require policy for effective enforcement.

Table 3.1. Socio-technical systems design principles, adopted from Cherns (1987)

STSD Principle	**Description**
Compatibility	The system must be designed to be compatible with organizational objectives.
Minimal Critical Specification	Design of the system must specify no more and no less than what is necessary.
Variance Control	Unprogrammed events must be controlled as close to their point of origin as possible.
Boundary Location	Boundaries must be drawn by technology, territory, and/or time to keep the processes pragmatic.
Information Flow	Design of the system must allow for information to be provided at the earliest possible point where action is needed.
Power and Authority	System designers must be free to respectfully use what they need and face ramifications if necessary.
Multifunctionality	The system must have the ability to be agile in adding new roles or modifying old ones.
Support Congruence	Social support systems must reinforce system objectives set by the organization.
Transitional Organization	The system design team must transition alongside organizational transitions.
Incompletion	The design process must start anew, with evaluation and new design follow implementation.

Government officials and citizens must use these principles to guide the creation of policies regarding the design and use of any E-Democratic Government systems. Specifically, policies must outline which E-Services are sought (compatibility), what the E-Services must do (minimal critical specification), how the E-Services must function (variance control, boundary location, information flow, and multifunctionality), how the E-Services will be administered (power and authority, support congruence, and transitional organization), and how the E-Services will be improved (incompletion). If these concepts are too abstract for practitioners, Lyytinen & Newman (2008) present a model of sociotechnical features to help bridge that divide consisting of four constructs: tasks, actors, structure, and technology, whereby tasks are the purposes of the system, actors are the stakeholders, structures are the arrangements by which the system operates, and technology refers to tools used to complete tasks.

After reviewing design collaboration literature to better inform this research and its deliverables, I note some common themes. First, the success of any design collaboration is at risk without agreement and clarity between government and citizens. For example, Lappas et al. (2015) conduct a survey to evaluate E-Government initiatives in Greece and find most citizens valued E-Government services that reduced bureaucracy or provided information, but that respondents were generally not ready for deliberative or participatory features. Accordingly, any deliberative or participatory features in an E-Democratic Government platform here would likely have failed due to low use rates. The failure to first assess needs and citizen sentiments in designing E-Government initiatives can single-handedly cause an initiative to fail to meet its objective. In another example, Prasad (2012) conducts case studies on two E-Government projects—the Indian Government's National E-Governance Plan (extended Internet to remote villages) and the Indian State of Kerala's *Akshaya Centres* project (policies and public-private partnerships which sought to increase e-literacy, capacity building, and installation of computer kiosks)—and finds that the latter proved significantly more influential on participation levels. This is because the biggest challenge to e-Participation here was not lack of internet access, but lack of device access and familiarity with technology.

Cases of disconnection between citizens and government may be exacerbated by the knowledge silo problem, where knowledge sharing is somehow restricted, e.g., through system incompatibility or disintegration, regulations, procedures, etc. (Mergel, 2010). To address this problem, this research recommends use of the model of collaboration in multisourcing information security by Naicker and Mafaiti (2019), where service providers, technology vendors, and clients share knowledge and vision through communication, coordination, and creation of formal structures for collaboration facilitated by the clients. In addition, this research recommends use of the model provided by Porwol et al. (2013), which integrates citizen-led and government-led participation processes and identifies requirements for e-Participation that would enable citizens to directly influence policy making. For citizen-led participation, government needs tools to: (a) facilitate processing of vast social media participation data; (b) interact effectively with citizens and shape discussion on deliberation platforms; and (c) monitor the social media and similar place of spontaneous citizens' deliberation. For government-led participation, government needs tools to: (d) facilitate the processing of participation data; (e) provide feedback to citizen's contributions; (f) dissemination and reaching wide audiences; and (g) a platform to invite people to participate and discuss issues (p. 291).

The experience of private organizations engaging with large communities online suggests that success is possible for the public sector with proper planning and implementation. Although I found no theories that directly relate to online community engagement from the public sector perspective, I found one publication that creates a theory explaining corporate organizations and their engagement practices with the open source Linux community. Germonprez et al. (2017) synthesize a theory called responsive design, guided by the principles of interconnection, opportunism, and domestication. In this context, interconnections are the high and low contributions to a community, representing the responsivity of organizations to communities; opportunism is the collective and bidirectional negotiation, open availability, and utilization of resources between the community and corporation; and domestication is the creation of a managed and stabilized environment that supports structured practices in corporate and communal artifact design (Germonprez et al., 2017, p. 70-75). This research recommends the use of these principles to guide the design of collaborative technologies, but admittedly, these principles are not very practical for E-democracy initiatives. In that regard, Hanson et al. (2019) recommend using reputational systems and their signals—namely point accrual systems (points), labeling systems (labels), or badging systems (badges)—as a means of increasing role clarity which, as their research shows, can drive greater engagement. Thus, this research also recommends the use of reputational systems and provides guidance on their design.

To maintain trust, E-Democracy initiatives need to be more than just inclusive; they also need to be secure and offer credible guarantees for user privacy. Accordingly, in developing the framework artifact, I will make sure that privacy concerns, especially transparency in privacy settings and tight default privacy settings, are integrated at every stage of design and implementation. However, in this project, it will only be possible to identify general or baseline privacy requirements since, in the interest of inclusivity and trust-building, each community's users will need to define what privacy means to their instantiation. Literature in both the technical and functional perspectives regarding defense-in-depth will be incorporated into the design of the framework artifact, as well as the artifact itself (Groat et al., 2012; Liu et al., 2015). Other specialty frameworks, such as the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (FFIEC, 2017), will be referenced as an example to incorporate similar features like mappings to other frameworks.

To further communicate this work to practitioners, I use lawsourcing for exemplifying the application of provided guidance in a synthetic platform due to its previous use in California state government and its compatibility with E-Democratic Government. Lawsourcing is the conceptual combination of the recent changes in the American legal environment and crowdsourcing—the crowdsourcing of legal proposals to achieve substantial legal reform and innovation. Lawsourcing is formally defined by Orozco (2016) as "an open call to online participants that requests their support to achieve a legal objective" (p. 154). Orozco (2016) clarifies that lawsourcing initiatives must: (1) provide more options than traditional law solutions using crowdsourcing principles; (2) offer access to the legal system at a much lower cost than traditional law solutions; and (3) serve to further disrupt the traditional legal environment (p. 154-159). Accordingly, lawsourcing is chosen as the basis of scenario creation as these requirements all comply with my definition of E-Democratic Government; a government lawsourcing service would aim to increase citizen engagement through the act of deliberatively creating legal proposals using technology.

To illustrate when it is appropriate to evaluate and reevaluate activities within the E-Democratic process, I offer a diagram in Figure 3.1 that aligns the information system design research process by Nunamaker et al. (1990) with a digital government success model by Gil-Garcia & Flores-Zúñiga (2020). Nunamaker et al. (1990) provide a model depicting how systems are involved within and throughout the research process, whereby researchers first construct a conceptual framework, then develop a system architecture, analyze and design the system, build the (prototype) system, and finally observe, evaluate the system, and repeat the process (p. 98). Gil-Garcia & Flores-Zúñiga (2020) present a comprehensive digital government success model focusing on implementation and adoption based on data from 32 states of Mexico, and the model consists of five stages: (1) external conditions, made up of political, social, and economic considerations; (2) implementation, including general organization characteristics and institutional arrangements; (3) supply, consisting only of digital government services; (4) adoption, including considerations of usefulness perception and ease of use perception; and (5) demand, consisting only of actual use of digital government services

(p. 5). As shown in Figure 3.1, evaluation and re-evaluation are recommended to occur during each stage to detect and remedy compliance issues as early as possible.

Trust in government (TGV), citizen engagement (CEN01), collaborative design through socio-technical theory (CEN02), computer security (SEC), and user privacy (PRV) all play a central role in determining the success of E-Democratic Government initiatives, and the artifact

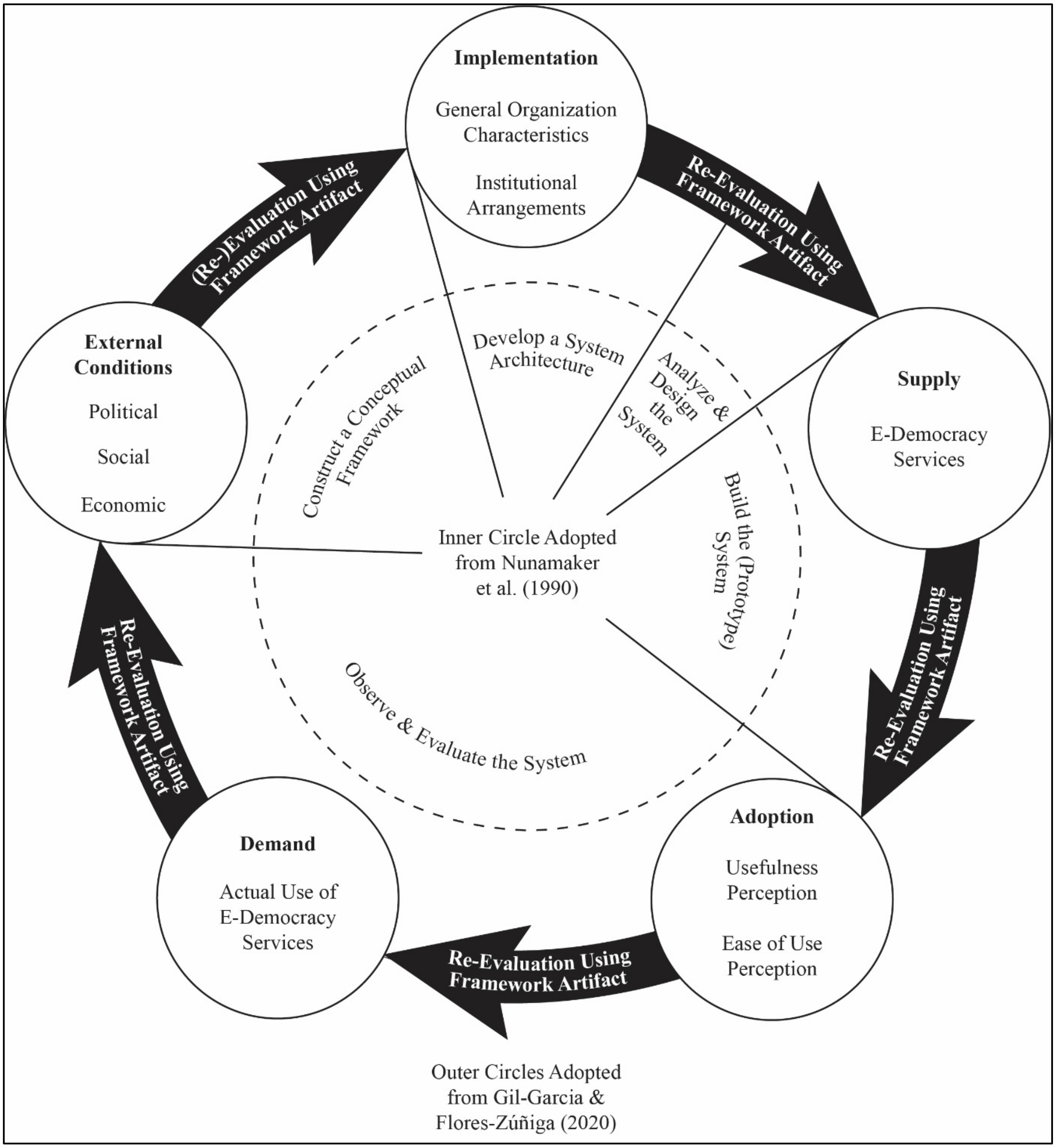
Implementation
General Organization Characteristics
Institutional Arrangements
Re-Evaluation Using Framework Artifact
Supply
E-Democracy Services
Re-Evaluation Using Framework Artifact
Adoption
Usefulness Perception
Ease of Use Perception
Re-Evaluation Using Framework Artifact
Demand
Actual Use of E-Democracy Services
Re-Evaluation Using Framework Artifact
External Conditions
Political
Social
Economic
(Re-)Evaluation Using Framework Artifact
Construct a Conceptual Framework
Develop a System Architecture
Analyze & Design the System
Build the (Prototype) System
Observe & Evaluate the System
Inner Circle Adopted from Nunamaker et al. (1990)
Outer Circles Adopted from Gil-Garcia & Flores-Zúñiga (2020)

Figure 3.1. Model of framework use

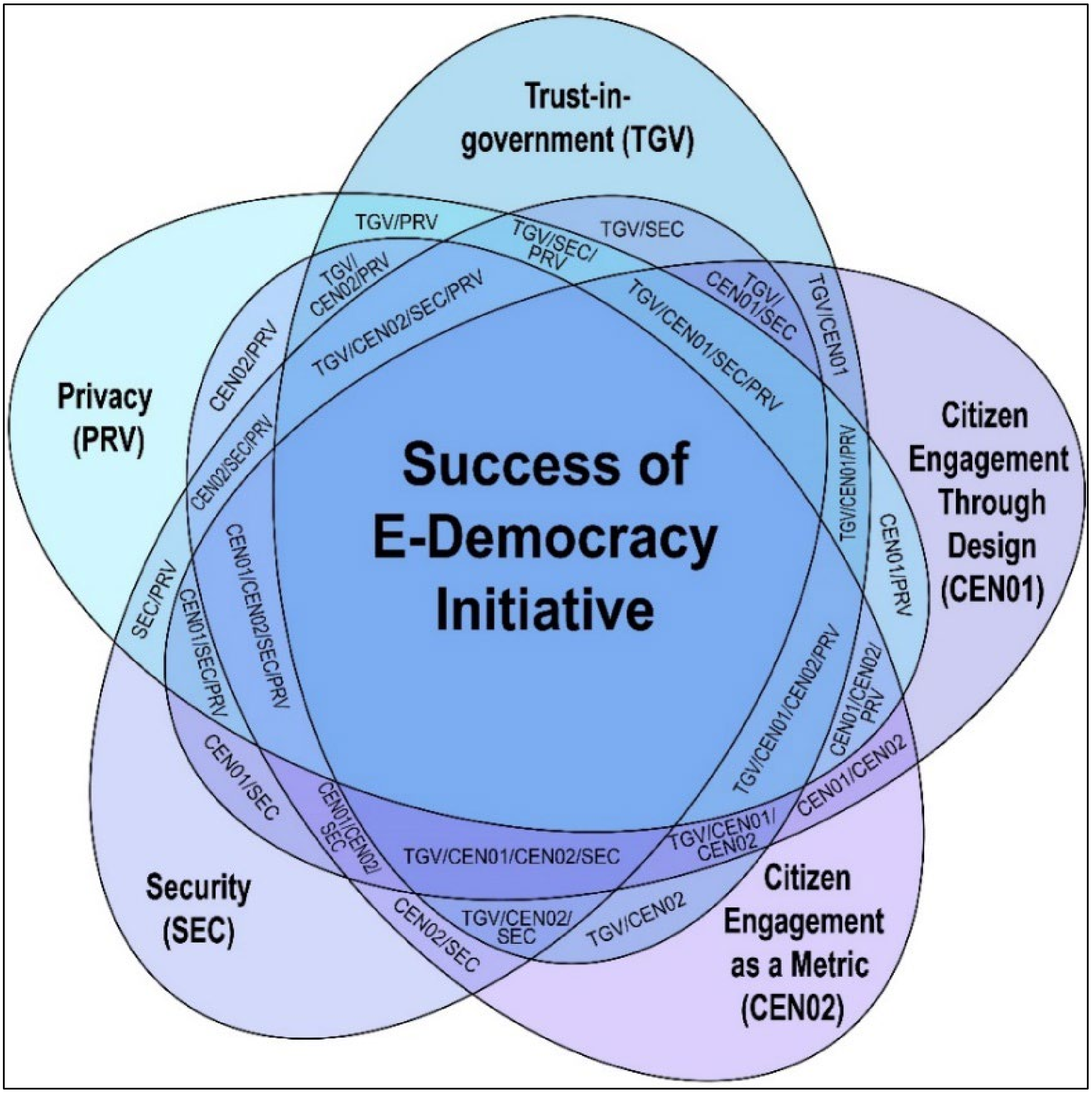

Figure 3.2. E-democracy success model

design considers each for this reason. This research is not concerned with the extent to which each factor increases the likelihood of E-Democratic Government success, but only with which factors the literature identifies as able to increase the likelihood of E-Democratic Government success. With no trust in government, citizens perceive no benefits associated with participating in E-Democratic Government. Without citizen engagement, it is difficult for government to justify further funding or support for such initiatives. Without integrating all stakeholders into the design process of E-Democratic Government initiatives, important social and organizational aspects are not considered, leading to lower engagement and satisfaction. And without computer security and user privacy, citizen information is prone to exposure and the purpose of an E-Democratic Government platform would quickly become infeasible. This research aims to communicate these principles in a concise and comprehensive manner to municipal leadership bodies in the US through applying provided guidance to a synthetic lawsourcing platform. To visually communicate this research's understanding of these factors and how they influence the success of E-Democratic Government initiatives, I offer a rudimentary model in Figure 3.2.

Implementation and validation methods

This research uses design science research (DSR) methodology to develop a holistic E-Democratic Government success framework for US municipalities. Specifically, I use Hevner et al.'s (2004) seven DSR guidelines to create a method artifact—loosely defined as an innovation that defines the processes for design, implementation, use, and evaluation of information systems to solve a problem—in offering E-Democratic Government as a solution to multi-decade declines in US local political engagement (p. 75-9). Table 3.2 presents how each guideline will be used to develop a rigorous, comprehensive, and effective framework informing success requirements for E-Democratic Government initiatives.

Hevner et al. (2004) define five categories of design evaluation methods: observational, analytical, experimental, testing, and descriptive (p. 86). For my dissertation, four of these categories—observational, analytical, testing evaluations, and controlled experiments—are infeasible without a participating government that is willing to adopt the otherwise unverified framework. The observational category explicitly requires use of the artifact which inherently requires a government due to the nature of this research. Similarly, the analytical and testing categories require some degree of the artifact's implementation, as analytical evaluation requires analyzing the artifact's behavior or practical performance, and testing evaluation requires executing artifact interfaces or implementing the artifact in full. Implementation is obviously not possible without a participating government. Similarly, a field experiment is also infeasible because it would again require some level of government participation (and other types of experiment conditions would lack external validity).

Table 3.2. DSR steps, adopted from Hevner et al. (2004)

Hevner et al. (2004) Guideline	Description
Design as an Artifact	Holistic e-democratic government success framework for US municipalities
Problem Relevance	Multi-decade declines in US local political engagement
Design Evaluation	Benchmarking between artifact, past e-democracy initiatives, and security standards; scenario creation via synthetic lawsourcing platform; and mapping redundancies of requirements, all using logical reasoning/informed argument where applicable
Research Contributions	Literature review spanning multiple relevant disciplines; theoretical contributions in E-Government, E-Democracy, deliberative democracy, trust in government, citizen engagement, sociotechnical theory, and decision support systems; artifact framework
Research Rigor	Utilization of multiple disciplines' theories and literature; incorporation of Hevner et al. (2004), Peffers et al. (2008), and Vaishnavi (2008) DSR guidance
Design as a Search Process	Incorporation of such a plethora of material allows the researcher to be selective in artifact design
Communication of Research	Eventual publication as dissertation, spurring future research publications

On the surface, simulation offers a viable strategy for my project, but I cannot find relevant data to facilitate simulation. Academic research suggests that simulation evaluation is possible when real-life setting validation is too costly or complex for mathematical proofs, and when it is possible to model the problem and solution using a computer (Vaishnavi, 2008). As the artifact is a framework of success requirements, accurately modeling the artifact on a computer as a solution requires input data as a problem. For example, if E-Government data measuring citizen trust, platform participation, perceived success, and other relevant metrics were provided, the data could be coded according to the framework's requirements to simulate whether compliance to the framework correlates with higher perceived success. However, I found no E-Government, E-Democracy, or trust in government publications that measure similar concepts and provide enough information to allow for simulation validation. AlSuwaidi & Rajan (2013) do not consider citizen trust, whereas Antoni et al. (2017) only look at trust and transparency but not security or privacy. Avgerou (2013) focuses only on E-voting considerations, while the model produced in Liu & Zhou (2010) only measures citizen perception. Further, most publications that offer a relevant model provide no additional mathematical analysis or validation (AlSuwaidi & Rajan, 2013; Altameem et al., 2006; Avgerou, 2013; Panda & Sahu, 2013; Supriyanto et al., 2019). Because this research does not have such an avenue, I cannot conduct an experimental evaluation in this project.

The only remaining feasible category of evaluation methods is the descriptive category. Vaishnavi (2008) and Hevner et al. (2004) agree that researchers should avoid using descriptive evaluation methods like logical reasoning and informed argument unless other methods cannot be readily employed. Hevner et al. (2004) write that "descriptive methods of evaluation should only be used for especially innovative artifacts for which other forms of evaluation may not be feasible" (p. 86). If one can interpret ‘especially innovative’ to include creating a method artifact in a research area where literature lacks models and relevant methodological support, my evaluation should certainly qualify. For an example of similar validation, Fraser & Vaishnavi (1997) use only logical reasoning to validate their capability maturity measurement model for software development environments’ formal specification processes. However, in acknowledging the perceived weakness of descriptive evaluation, I use multiple descriptive evaluation methods to improve the strength of evaluation.

Vaishnavi (2008) defines benchmarking as the use of “an available benchmark to show that one’s solution has reasonable performance or is better than some other available solution” (p. 167). As Hevner et al. (2004) defines using information from the knowledge base to build a convincing argument for an artifact’s validity, I consider benchmarking to be a subset of informed argument validation. The process of benchmarking includes identifying the benchmark (or creating and verifying your own) and then using the benchmark to demonstrate the effectiveness of the proposed solution versus existing ones. In this case, I identify past E-Democracy initiatives and relevant cybersecurity frameworks as the most applicable benchmarks for comparison, and I map the artifact to these benchmarks.

Scenarios are the other descriptive evaluation method identified by Hevner et al. (2004). Peffers et al. (2012) identify illustrative scenarios as one of the most used evaluation methods and further define illustrative scenarios as applying “the artifact in a synthetic or real world simulation to demonstrate its utility” (p. 4). In this research, I identify lawsourcing as an avenue to communicate the artifact’s requirements more clearly to practitioners, as lawsourcing is an easier concept to understand than E-Democratic Government itself. Accordingly, I apply the artifact’s requirements to a synthetic lawsourcing platform.

Finally, defense in depth theory is not a benchmark, but rather a methodology of cybersecurity that calls for a balanced focus between people, technology, and operations through clear accountability, thorough documentation, and layering through redundancy (US National Security Agency, 2015). I apply defense in depth theory to the artifact as informed argument evaluation, as it is certainly descriptive in nature but does not illustrate a scenario. As defense in depth theory was used both in the artifact design and provided guidance, I provide evaluation of how the artifact's requirements support or are interrelated to each other (US National Security Agency, 2015).

To further clarify this work in a DSR context, Figure 3.3 presents this research according to the Design Science Research Methodology from Peffers et al. (2008). The authors' model depicts six activities (identify problem and motivate, define objectives of a solution, design and development, demonstration, evaluation, and communication) and four possible research entry points in DSR: problem-centered initiation, objective-centered solution, design and development centered initiation, and client/context initiated. Each of the six activities' descriptions for this research can be found above. Although a case can be made that this research may be considered objective-centered, I ultimately labeled this research as taking a problem-centered approach. This is because Peffers et al. (2008) clarify that, in problem-oriented DSR approaches, "the idea for the research resulted from observation of the problem or from suggested future research in a paper from a prior project," whereas objective-centered solutions "could be triggered by an industry or research need that can be addressed by developing an artifact" (p. 56). In this case, the initial idea for this research project stemmed from Orozco's (2016) call for the public sector to bridge the gap in E-Services as compared to the private sector. Although the research and practical need for increasing civic engagement in local US politics became the ultimate motivation behind this research, this discovery came after the initial research idea.

In conclusion, to evaluate the artifact, I compare the artifact to two benchmarks—past E-Democracy initiatives in the US and relevant cybersecurity frameworks; I apply defense in depth theory as an additional means of informed argument; and I create an illustrative scenario where the artifact's requirements are applied to a synthetic lawsourcing initiative.

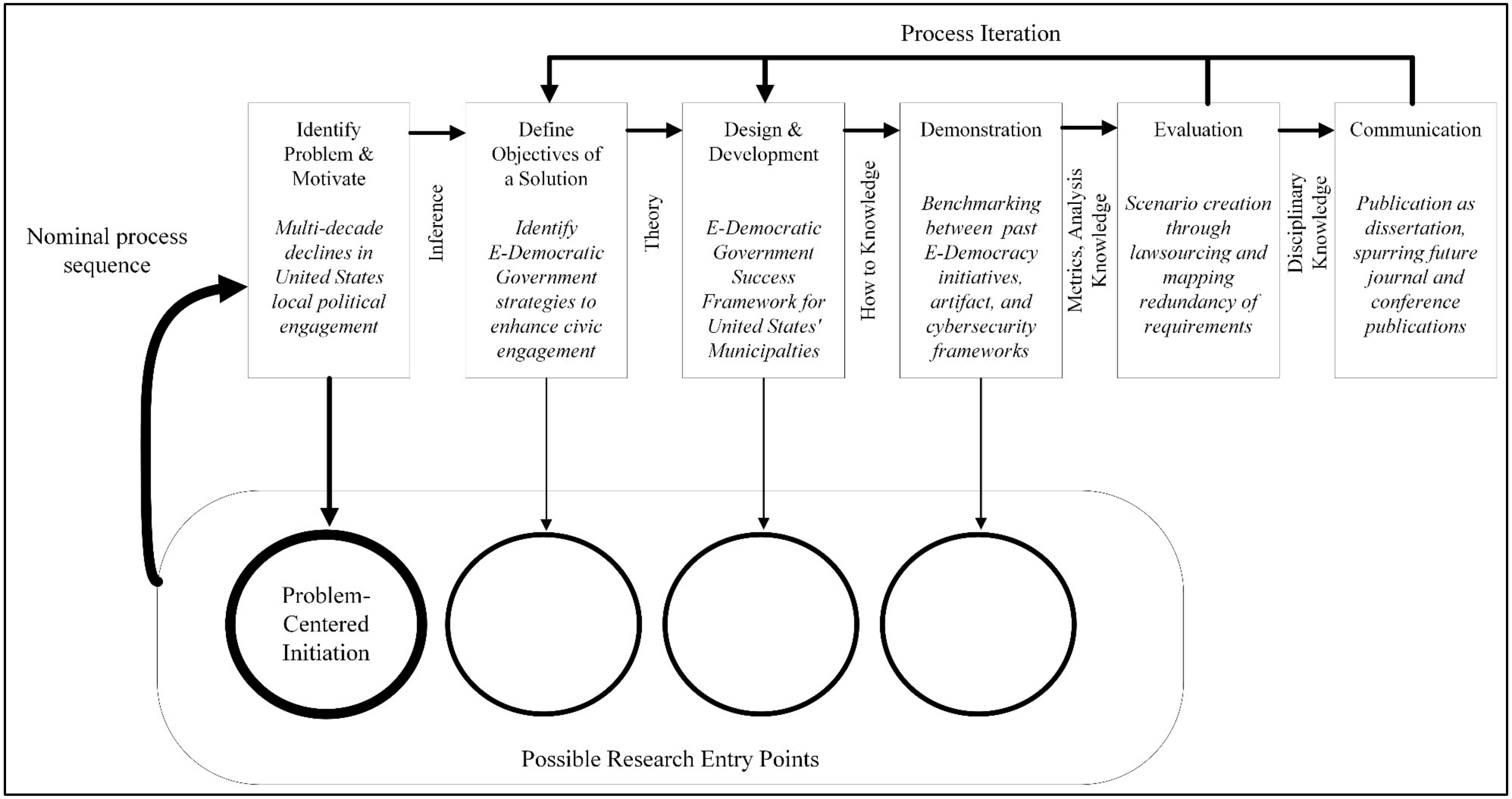
Process Iteration
Nominal process sequence
Identify Problem & Motivate
Multi-decade declines in United States local political engagement
Inference
Define Objectives of a Solution
Identify E-Democratic Government strategies to enhance civic engagement
Theory
Design & Development
E-Democratic Government Success Framework for United States' Municipalties
How to Knowledge
Demonstration
Benchmarking between past E-Democracy initiatives, artifact, and cybersecurity frameworks
Metrics, Analysis Knowledge
Evaluation
Scenario creation through lawsourcing and mapping redundancy of requirements
Disciplinary Knowledge
Communication
Publication as dissertation, spurring future journal and conference publications
Problem-Centered Initiation
Possible Research Entry Points

Figure 3.3. Design science research methodology, adopted from Peffers et al. (2008)

CHAPTER 4

RESULTS

E-Democratic Government Success Framework for United States' Municipalities

PART ONE — INTRODUCTION

PURPOSE STATEMENT

The purpose of this framework is to address the problem of low citizen engagement in US municipal politics through providing guidance that informs the requirements, design, implementation, adoption, and evaluation of any E-Democratic Government initiative within this framework's scope, defined below. This framework aims to increase the prevalence and success of E-Democratic Government initiatives in US municipal politics.

BACKGROUND

Citizen engagement in US municipal politics is limited, even though citizens are impacted by the actions of local government to a much greater extent than those of the federal and state governments (Holbrook & Weinschenk, 2019). While some relatively new democracies have successfully implemented E-Democracy platforms or initiatives, like Brazil's *E-Democracia* platform (https://edemocracia.camara.leg.br/) and Estonia's Digital Society initiative (https://e-estonia.com/), the US has yet to make meaningful strides in E-Democracy (Orozco, 2016).

E-Government presents a possible solution to the challenges of low participation in local politics, as use of E-Government can increase citizens' trust, interactions, and perceived responsiveness with government (Tolbert & Mossberger, 2006). The terms E-Government, Digital Government, E-Governance, and E-Democracy are often used interchangeably in scholarly literature. Agawu (2017) defines E-Government as, "the delivery of government information and services online through the Internet or other digital means" (p. 3). The breadth of this definition needs further refinement before adopting for use to exclude initiatives that do not increase democratic engagement. Orozco (2016) defines E-Democracy as "the digitization of decision making processes regulated by law and increasing citizen engagement in civic and political activity through the use of technology" (p. 163). This definition aligns with the purpose statement but excludes initiatives that do not digitize decision making processes.

As the purpose statement seeks to include initiatives that do not directly digitize decision making but nonetheless contribute to furthering citizen engagement (e.g., citizen learning, decision support, etc.), I suggest a hybrid term to adopt. Borrowing from Agawu (2017) and Orozco (2016), I define E-Democratic Government as the digital or online means for delivering government information and services with an aim to increase citizen engagement in civic, deliberative, and political activity through the use of technology.

SCOPE

This framework makes extensive use of the word "initiative" regarding the E-Democratic Government product that users are guided towards designing, implementing, adopting, and/or evaluating. This framework only considers initiative success from the government-to-citizen (G2C) perspective, and requires that such an initiative, at minimum: (1) complies with the Orozco (2016) definition of E-Democracy, which inherently requires use or intended use of at least one system for the purpose of digitizing decision making processes and/or increasing citizen engagement in civic, deliberative, and political activity; and (2) meets at least the baseline standard of the E-Government G2C Trends per Agawu (2017) success requirement of the framework. If an initiative does not meet both requirements, it falls outside the scope of this framework.

In this case, the initiative is assumed to be operated and managed by citizens in a US municipality within or outside of government for the purpose of increasing civic engagement. However, E-Democratic Government initiatives occurring elsewhere could still use the guidance offered in this framework, with the understanding that discrepancies are inevitable. Because small governments, individuals, and not-for-profit organizations are the most likely users, some of the baseline standards of the framework's success requirements may be difficult, if not impossible to achieve without sufficient resources. When an insufficient number of resources are available, users must identify which requirements are infeasible, determine a feasible alternative baseline standard that is relevant to the success requirement, and justify its substitution to the target jurisdiction's community. However, none of the intermediate or innovative standards can be substituted in this way. Also, the scope requirements cannot be substituted or changed in any way.

TARGET AUDIENCE

This framework was designed for use by: (1) public government officials and/or employees in United States' municipalities who are authorized to start, design, plan, manage, and/or evaluate E-Democratic Government initiatives; (2) citizens and/or third parties who wish to evaluate or propose E-Democratic Government initiatives; and (3) researchers as a contribution towards the larger research agenda that considers the integration of information communication technologies into the policymaking process. When lack of resources makes meeting the baseline standards of requirements untenable, users must identify which requirements are infeasible, determine a feasible alternative baseline standard that is relevant to the success requirement, and justify its substitution to the target jurisdiction's community. However, none of the intermediate or innovative standards can be substituted in this way.

HOW TO USE THE FRAMEWORK

This framework consists of: (1) descriptions of each success requirement; (2) a table listing each of the success requirements' baseline, intermediate, and innovative standards for compliance with this framework; and (3) a table listing each of the success requirements, internally related requirements of each, and external literature used to help inform each requirement.

The Model of Framework Use (Figure 3.1) is a depiction of when evaluation/re-evaluation of the initiative using this framework should occur, against both the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), as well as the System Development Research Process from Nunamaker et al. (1990). If there is no existing initiative, initial evaluation using the framework should begin after identification of external conditions has occurred. The E-Democracy Success Model (Figure 3.2) is offered as a preliminary model and visual aid to illustrate the five categories of success identified in this research, listed below, and their interrelatedness.

The process of starting, designing, planning, managing, and/or evaluating an E-Democratic Government initiative using the framework is a qualitative, inherently subjective process, and requires an honest mapping of the initiative to each of the framework's standards.

If the baseline standard for any one requirement is not met, the initiative is noncompliant with said requirement and accordingly risks the initiative's success. However, noncompliance in one or more other success requirements is expected, as the only disqualifying instance of noncompliance can occur in this framework's scope requirements.

RELATIONSHIP TO OTHER PUBLICATIONS

This framework maps numerous success requirements in the categories of E-Democracy trends, trust in government (TGV), citizen engagement (CEN), security (SEC), and privacy (PRV)—including three government-to-citizen (G2C) E-Government trends from Agawu (2017); three trust in government constructs from Papp et al. (2020); ten sociotechnical systems design requirements from Cherns (1987); seven voter decision support system requirements from Robertson (2005); security frameworks such as NIST SP 800-53 (NIST Task Force, 2020), the NIST Cybersecurity Framework (Barrett, 2018), and the McCumber Cube model (McCumber, 2004); and four privacy areas from Gerber et al. (2018). Other external publications used in the creation of the framework's requirements are cited in each requirement's description and/or standard, as well as summarized in the table, E-DEMOCRATIC GOVERNMENT SUCCESS REQUIREMENTS: INTERNALLY RELATED REQUIREMENTS AND SUPPORTING LITERATURE.

PART TWO — DESCRIPTIONS

Table 4.1. Descriptions of e-democratic government success requirements

E-Democratic Government Success Requirements	**Description**
E-Government G2C Trends per Agawu (2017)	Agawu (2017) refines government-to-citizen (G2C) E-Government activity by proposing three trends: (1) increasing access to information, which is the use of digital platforms or services to facilitate citizen access to relevant content; (2) digitizing the service loop, which is the process of digitizing some element of the government service while leaving the essential function unchanged; and (3) expansion or creation of new governance function, which is the use of technology to expand or create a government service that cannot readily be said to have a non-digital parallel (p. 3). At least one of these trends must be meaningfully present in an initiative to comply with this requirement. If an initiative is noncompliant with this requirement, it falls outside the scope of this framework.
Trust In Government (TGV) per Papp et al. (2020)	Trust in government is a moving target because citizens evaluate the credibility and reliability of government along three interconnected dimensions: (1) behavioral trust, or citizens' perceptions of the congruence between the behavior and personal characteristics of government officials, and the trust need of citizens; (2) operational trust, or citizens' perceptions of the congruence between the interactions of citizens with government and the outcomes that are expected from those interactions; and (3) institutional trust, or citizens' perceptions of the congruence between the actions, policies, and/or regulations of governmental institutions and/or their agents, and the citizens' expectations of those institutions and/or agents (Thomas, 1998; Tolbert & Mossberger, 2006; Tassabehji et al., 2007; Aladwani & Dwivedi, 2018; Papp et al., 2020). This category is critical to an initiative's success due to research showing a strong link between citizens' attitudes, beliefs, and E-Services utilization (Hossan & Ryan, 2018), as well as citizens' prior experiences, environmental conditions, and their perceptions of trust in government (Avgerou, 2013; Gil-Garcia & Flores-Zúñiga, 2020). The collection, measurement, analysis, evaluation, and interpretation of citizen trust in government sentiments are each critical to the success of any E-Democracy initiative and must be conducted as an ongoing process. Users must continually improve the means of collection, measurement, analysis, evaluation, and interpretation of citizen trust in government sentiments, not only by changing government but governance. For example, an anecdote from literature suggests the only significant connection between trust in government and interactions with politicians on social networking sites is the citizens' evaluation of likeability— not leadership, responsiveness, or benevolence alone (Starke et al., 2020, p. 6). Collecting, measuring, evaluating, and/or interpreting trust in government sentiments is likely to be challenging when an initiative is in development or infancy. Surveys, town hall meetings, and other means of polling constituents are recommended at this stage to ascertain trust requirements of any initiative. If initial participation is low, several products/methods exist that allow for sentiment analysis of trust through social media (see Calderon et al., 2015; Jaidka & Ahmed, 2015; Jamal et al., 2015; Papp et al., 2020; Starke et al., 2020). Users must also continually aim their initiative(s) towards the intermediate and innovative standards, which require predicting trust in government sentiments to some degree in further informing government and governance. Innovation in this realm is denoted by the ability to predict trust in government sentiments accurately and reliably based on the personal characteristics of government officials; interactions

E-Democratic Government Success Requirements	**Description**
	of citizens with government; and/or actions, policies, regulations, etc., of governmental institutions, and/or their agents (Tolbert & Mossberger, 2006; Papp et al., 2020). Because more research is needed in this area, it is recommended for users managing initiatives to supersede this guidance and conduct their own research in modeling trust in government as it pertains to their own constituents (e.g., Supriyanto et al., 2019). Due to lack of literature informing how these variables may appear in practice, the NICE Framework (NIST SP 800-181), a guide for creating cybersecurity workforce frameworks, is applied to each of the three dimensions of trust in government to envision what tasks, knowledge, and skills would be required at each standard (Petersen et al., 2020). Accordingly, knowledge and skill statements should be used as a recruitment standard for relevant trust in government support roles for any initiative, and task statements should be used as an assessment standard for those roles.
TGV01: Behavioral trust	Behavioral trust is the citizens' perceptions of the congruence between the behavior and personal characteristics of government officials, and the trust need of citizens (Thomas, 1998; Tolbert & Mossberger, 2006; Tassabehji et al., 2007; Aladwani & Dwivedi, 2018; Papp et al., 2020). Behavioral trust can be split into two categories: content-based trust, which is dependent on content meaningfulness, and engagement-based trust, which is dependent on interaction engagingness (Aladwani & Dwivedi, 2018, p. 263-268). Because the natures of trust in government, content meaningfulness, and interaction engagingness are based on the citizen perspective instead of actual trust, success depends on fully understanding citizen trust in government sentiments through their collection, measurement, analysis, evaluation, and interpretation—in this category, especially as it relates to elected government officials who will inevitably be up for reelection. Preliminary research in this area indicates that both positive and negative citizen expression of trust in government sentiments may be largely skewed towards behavioral trust sentiments on social media (Papp et al., 2020).
TGV01.1: Tasks	Required tasks are comprised of varying levels of the collection, measurement, analysis, evaluation, interpretation, and in later standards, prediction of citizen trust in government data regarding government officials' personal characteristics. Relatedly, tasks also include the alignment of initiative data to governance through assessing the personal characteristics of government officials.
TGV01.2: Knowledge	Required knowledge in the baseline standard includes understanding of appropriate data collection, measurement, analysis, and evaluation techniques, the context of citizens' external conditions (previous experiences—political, social, and economic) and how to interpret citizen trust in government data into empirically evidenced findings. In the later standards, required knowledge also includes data prediction techniques and understanding complex knowledge management systems that optimize and automate the data collection, measurement, analysis, evaluation, and interpretation of citizen trust in government data.
TGV01.3: Skills	Required skills include the abilities to appropriately conduct data collection, measurement, analysis, evaluation, interpretation, and in later stages, prediction; to navigate and adapt government and its officials; and to communicate with and appropriately respond to citizens and other government officials.

E-Democratic Government Success Requirements	**Description**
TGV02: Operational trust	Operational trust is the citizens' perceptions of the congruence between the interactions of citizens with government and the outcomes that are expected from those interactions (Thomas, 1998; Tolbert & Mossberger, 2006; Tassabehji et al., 2007; Aladwani & Dwivedi, 2018; Papp et al., 2020). Operational trust is produced through repeated exchanges rather than one-time experiences, and accordingly emerges over time (Thomas, 1998). Operational trust can be gained/lost by entire organizations as well as by individuals within those organizations and is entirely dependent on the processes administered by government intended for citizens, the outcomes of those processes, and the expectations of the citizens (Tassabehji et al., 2007). Responsive design through the following theoretical principles is recommended for use to help bridge the gap between government and citizens: (1) interconnection, or reflection of organizational roles in balancing contribution and differentiation at the interface of organizational and communal efforts; (2) opportunism, or the collective and bidirectional negotiation, open availability, and utilization of resources between the community and organization; and (3) domestication, or the creation of a managed and stabilized environment that supports structured practices in organizational and communal artifact design (Germonprez et al., 2017). Operational trust can be split into two categories: content-based trust, which is dependent on content meaningfulness, and engagement-based trust, which is dependent on interaction engagingness (Aladwani & Dwivedi, 2018, p. 263-268). Because the natures of trust in government, content meaningfulness, and interaction engagingness are based on the citizen perspective instead of actual trust, success depends on fully understanding citizen trust in government sentiments through their collection, measurement, analysis, evaluation, and interpretation.
TGV02.1: Tasks	Required tasks are comprised of varying levels of the collection, measurement, analysis, evaluation, interpretation, and in later standards, prediction of citizen trust in government data regarding government processes. Relatedly, tasks also include the alignment of initiative data to governance through assessing government processes.
TGV02.2: Knowledge	Required knowledge in the baseline standard includes understanding of appropriate data collection, measurement, analysis, and evaluation techniques, the context of citizens' external conditions (previous experiences—political, social, and economic) and how to interpret citizen trust in government data into empirically evidenced findings. In the later standards, required knowledge also includes data prediction techniques and understanding complex knowledge management systems that optimize and automate the data collection, measurement, analysis, evaluation, and interpretation of citizen trust in government data.
TGV02.3: Skills	Required skills include the abilities to appropriately conduct data collection, measurement, analysis, evaluation, interpretation, and in later stages, prediction; to navigate and adapt government and its officials; and to communicate with and appropriately respond to citizens and other government officials.
TGV03: Institutional trust	Institutional trust is the citizens' perceptions of the congruence between the interactions of citizens with government institutions and/or their agents, the actions, policies, and/or regulations of governmental institutions and/or their agents (Thomas, 1998; Tolbert & Mossberger, 2006; Tassabehji et al., 2007; Aladwani & Dwivedi, 2018; Papp et al., 2020). Institutional trust can be split into two categories: content-based trust, which is dependent on content meaningfulness, and engagement-based trust, which is dependent on interaction engagingness (Aladwani & Dwivedi, 2018, p. 263-268). Because the natures of trust in government, content meaningfulness, and interaction engagingness are based on the citizen perspective instead of actual trust, success depends on fully understanding citizen trust in government sentiments through their collection, measurement, analysis, evaluation, and interpretation.

E-Democratic Government Success Requirements	**Description**
TGV03.1: Tasks	Required tasks are comprised of varying levels of the collection, measurement, analysis, evaluation, interpretation, and in later standards, prediction of citizen trust in government data regarding actions, policies, and/or regulations of governmental institutions and/or their agents. Relatedly, tasks also include the alignment of initiative data to governance through assessing actions, policies, and/or regulations of governmental institutions and/or their agents.
TGV03.2: Knowledge	Required knowledge in the baseline standard includes understanding of appropriate data collection, measurement, analysis, and evaluation techniques, the context of citizens' external conditions (previous experiences—political, social, and economic) and how to interpret citizen trust in government data into empirically evidenced findings. In the later standards, required knowledge also includes data prediction techniques and understanding complex knowledge management systems that optimize and automate the data collection, measurement, analysis, evaluation, and interpretation of citizen trust in government data.
TGV03.3: Skills	Required skills include the abilities to appropriately conduct data collection, measurement, analysis, evaluation, interpretation, and in later stages, prediction; to navigate and adapt government and its officials; and to communicate with and appropriately respond to citizens and other government officials.
Citizen Engagement (CEN)	Citizen engagement is defined by Olphert & Damodaran (2007) as "the active participation of citizens, in partnership with government, in decision and policy making processes" (p. 494). Batlle-Montserrat et al. (2014) identify citizens' engagement as one of nine categories of the most important services provided by public administrations, and describe citizens' engagement as including: (1) the satisfaction of citizens' expectations; (2) the attraction of citizens' attention; (3) the consolidation of bonds between citizens and government; (4) the encouragement of the relationship between citizens and their administrations; and (5) the promotion of or participation in E-Democracy activities by both parties (p. 62). Adopted from these definitions, this framework assesses citizen engagement from two perspectives: citizen engagement through design and citizen engagement as a success metric. Several pieces of literature not only advocate for citizen engagement in the design process but also to be used as a metric of success and user commitment/loyalty (Olphert & Damodaran, 2007; Bateman et al., 2011). E-Services must be designed for equal accessibility and operability to be perceived as legitimately seeking more engagement (Bonacin et al., 2009; Hansson et al., 2014). Hansson et al. (2014) have developed software for group collaboration that generates, reports, and updates a participation score for each user in real time to reveal any power imbalances, and the software is designed according to the following criteria: (1) participants are equal members; (2) participants set the agenda together; (3) participants can fully participate in the discussion; (4) all participants have the same status when decisions are taken; and (5) everyone has an enlightened understanding of the discussion. This framework also requires systems and processes to adhere to these criteria. This framework enforces compliance with these criteria by requiring compliance with sociotechnical theory principles during design of initiatives (Cherns, 1987), and by requiring compliance with decision support systems requirements for voting systems (Robertson, 2005).
CEN01: Design using STT per Cherns (1987)	Sociotechnical theory assumes that organizational objectives are best met by the joint optimization of the social and technical aspects, rather than forcing societal systems to adapt to technological optimizations (Cherns, 1976; Clegg, 2000). Sociotechnical system design (STSD) is defined as "an approach to design that consider human, social and organizational systems" (Baxter & Sommerville, 2011, p. 4). Other definitions in literature appear to be sympathetic towards this definition with minor deviations (Ayyad, 2017; Cherns, 1976;

E-Democratic Government Success Requirements	**Description**
	Cherns, 1987; Clegg, 2000; Lyytinen & Newman, 2008; Hapsara, 2016). Accordingly, this framework uses the Cherns (1987) ten STSD principles as CEN01.x requirements for the citizen engagement by design, while using Cherns (1976) and Clegg (2000) where necessary for support in some of the more detailed elaborations of the principles.
CEN01.1: Compatibility	The principle of compatibility requires the design process of the initiative system to be compatible with the objectives of the initiative (Cherns, 1987, p. 154-155). Assuming the initiative system is within the scope of this framework, it is required to, at minimum: (1) use at least one system for the purpose of digitizing decision-making processes and/or increasing citizen engagement and (2) meet the baseline standard of the E-Government G2C Trends success requirement of this framework. Grönlund (2003) classifies democratic decision making processes through a policymaking cycle model, starting with: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and ending with (5) monitoring the policy (p. 95). Therefore, to comply with the baseline standard of this requirement, the initiative must complete or meaningfully initiate digitization for at least one of these stages of policymaking and must also increase access to information using digital services to facilitate citizen access to relevant content, digitize the service loop, and/or expand or create governance function through technology. To comply with the intermediate and innovative standards of this requirement, initiatives must complete digitization of progressively more stages of the policymaking cycle, enable citizen learning, and use knowledge management research to help prevent knowledge silo issues and automate the policymaking stages (Mergel, 2010; Nemati et al., 2002; Porwol et al., 2013).
CEN01.2: Minimal critical specification	The principle of minimal critical specification requires that the tasks, allocation of tasks to jobs, and allocation of jobs to roles within the initiative system must specify: (1) no more than what is essential, and (2) no less than what is essential (Cherns, 1987, p. 155). In all standards of this requirement, this framework enforces compliance of these requirements through requiring mapping of tasks, knowledge, and skills of each workforce role per the NICE Framework (NIST SP 800-181; Petersen et al., 2020). For the intermediate and innovative standards of this requirement, this framework requires the use of the model provided by Porwol et al. (2013), which integrates citizen-led and government-led participation processes and identifies requirements for e-Participation that would enable citizens to directly influence policy making. According to the authors, for citizen-led participation, government needs tools to: (a) facilitate processing of vast social media participation data; (b) interact effectively with citizens and shape discussion on deliberation platforms; and (c) monitor the social media and similar places of spontaneous citizens' deliberation. For government-led participation, government needs tools to: (d) facilitate the processing of participation data; (e) provide feedback to citizen's contributions; (f) dissemination and reaching wide audiences; and (g) a platform to invite people to participate and discuss issues (Porwol et al., 2013, p. 291).
CEN01.3: Variance control	The principle of variance control (formerly 'the sociotechnical criterion') requires that variances in the initiative system must not be exported across bureaucratic or social boundaries (Cherns 1987, p. 156). This principle aligns with the NIST Cybersecurity Framework's Detect function, where anomalies and events, security continuous monitoring, and detection processes are required to prevent variances wherever possible (Barrett, 2018). Variance control also aligns with NIST SP 800-53 control AC-5 (separation of duties), which requires "dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions" (NIST Joint Task Force, 2020, p. 36). Variance control echoes the criteria for democratic systems given by Hansson et al. (2014), in that participants need to be equal members regardless of bureaucratic or social boundaries, and that all participants have the

E-Democratic Government Success Requirements	Description
	same status when decisions are taken. Although the success requirement *CEN01.6: Power and authority* contradicts the idea that all participants are equal members, this conflict is addressed by the democratic election of those in higher power/authority than typical users. Antoni et al. (2017) define transparency in E-Government as "a principle that guarantees or gives freedom to every person who requires to obtain information about the implementation of government in terms of policy, the process of making and its application and the results achieved or the open policy of supervision" (p. 2). Accordingly, innovation in this requirement is demonstrated through transparency of public user contributions to the initiative system and how they affect policy making, implementation, and outcomes.
CEN01.4: Boundary location	The principle of boundary location requires that initiative system boundaries must not be drawn as to impede the sharing of information, knowledge, and/or learning (Cherns, 1987, p. 156). This coincides with Davis's (1989) definition of perceived usefulness, which specifies that people tend to use or not use an application to the extent they believe it will help them perform their job better. Accordingly, this framework requires initiative system boundaries be drawn to facilitate, and not hinder, the sharing of information, knowledge, and/or learning. Bateman et al. (2011) find that users' needs, affects, and/or obligations can be predictive of which behaviors they will exhibit, with need-based commitment predicting thread reading, affect-based commitment predicting reply posting and moderating behaviors, and obligation-based commitment predicting moderating behavior. Naicker and Mafaiti (2019) offer a model for collaboration in multisourcing information security where service providers, technology vendors, and clients share knowledge and vision through communication, coordination, and creation of formal structures for collaboration facilitated by the clients. Innovation in this requirement is demonstrated by the modeling of community commitment as in Bateman et al. (2011) and information security multisourcing as in Naicker & Mafaiti (2019).
CEN01.5: Information flow	The principle of information flow requires that information be provided to those who require it when they require it, and the principle also prohibits the interruption of information and insertion of information loops by misplaced boundaries (Cherns, 1987, p. 157). This principle aligns with NIST SP 800-53 control AC-4 (information flow enforcement), which requires enforcement of approved authorizations for controlling the flow of information within the system and between connected systems based on organizational policies pertaining to information flow (NIST Joint Task Force, 2020, p. 28). According to Baxter & Sommerville (2011), information flow considerations accompany both system engineering activities (procurement, analysis, construction, and operation) and the organizational change process (goal setting, process mapping, process design, process execution). Accordingly, this framework requires mapping information flow in both system engineering and organizational structures. As a starting point, Porwol et al. (2013) offer a Social Software Infrastructure model through which information flow between citizens and decision makers is illustrated. Antoni et al. (2017) define transparency in E-Government as "a principle that guarantees or gives freedom to every person who requires to obtain information about the implementation of government in terms of policy, the process of making and its application and the results achieved or the open policy of supervision" (p. 2). Innovation in this requirement is demonstrated through modeling information flow across system engineering and organizational structures, as well as transparency of information flows.

E-Democratic Government Success Requirements	**Description**
CEN01.6: Power and authority	The principle of power and authority requires that those who need resources to carry out their responsibilities should have access to those resources, have authority to command those resources, and accept responsibility for the prudent and economical use of those resources (Cherns, 1987, p. 157). This principle aligns with NIST SP 800-53 controls AC-6 (least privilege), which requires that the only authorized accesses allowed for users or processes are the ones that are necessary to accomplish assigned organizational tasks, and AU-10 (non-repudiation), which requires the organization to have the ability to provide irrefutable evidence that an individual or process has performed any action (NIST Joint Task Force, 2020, p. 36-103). However, to abide by the Hansson et al. (2014) democratic criteria, all participants must be both equal members and must have the same status when decisions are taken. To reconcile this contradiction, participants should democratically elect members to short-term leadership positions that hold higher power and authority in the initiative system than most users. However, the initiative must also abide by NIST SP 800-53 control AC-5 (separation of duties), which requires "dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions" (NIST Joint Task Force, 2020, p. 36). Accordingly, these democratically elected power users must not concurrently be users of the platform. Antoni et al. (2017) define transparency in E-Government as "a principle that guarantees or gives freedom to every person who requires to obtain information about the implementation of government in terms of policy, the process of making and its application and the results achieved or the open policy of supervision" (p. 2). Accordingly, innovation in this requirement is demonstrated through transparency of power and authority of initiative systems.
CEN01.7: Multifunctionality	The principle of multifunctionality requires that the initiative system and organization can add new roles or modify old roles. (Cherns, 1976, p. 787-788; Cherns, 1987, p. 158). In the spirit of sociotechnical theory, the users should be included within the decision making process of adding new roles and modifying old roles. Further, the necessity of adding and modifying roles should be expected per the agile development method. Although the need for these changes could stem from a vast number of causes, user acceptability and compatibility should always be the primary drivers of change (Davis, 1989; Porwol et al., 2013). Due to the lack of research informing how these variables may appear in practice, the NICE Framework, a guide for creating cybersecurity workforce frameworks, must be applied to envision what tasks, knowledge, and skills would be required to match emerging organizational, governmental, and/or constituent needs (Petersen et al., 2020). Accordingly, knowledge and skill statements should be used as a recruitment standard for relevant support roles for any initiative, and task statements should be used as an assessment standard for those roles.
CEN01.8: Support congruence	The principle of support congruence requires that the systems of social support should be designed to reinforce the behaviors which the initiative is designed to elicit (Cherns, 1976, p. 790). Put simply, social support systems for the initiative system must encourage citizen engagement. Cherns (1976) gives an example of how, if an organization is team-oriented, yet implements a payment system that only considers individual members, the payment system is incongruent to the objectives of the organization. In the case of E-Democratic Government, roles and functions that support the initiative must be compatible with the objectives of the organization. As the *CEN01.1: Compatibility* requirement addresses compatibility concerns in the design process, this requirement addresses compatibility concerns in the systems, roles, and functions that are in support of the initiative. Compliance with this requirement also ensures adherence to the policymaking stages from Grönlund (2003), described in *CEN01.1: Compatibility*.

E-Democratic Government Success Requirements	**Description**
CEN01.9: Transitional organization	The principle of transitional organization requires the planning and design of any initiative transitions before they occur (Cherns, 1987, p. 159). This principle complicates the innovative standard of success requirement *CEN01.7: Multifunctionality*, where users can create and modify their own roles within the initiative system. However, user changes to the initiative system and/or organizational structure can be anticipated and accorded for within the planning and design of the original initiative system. This principle aligns with success requirements *CEN01.2: Minimal critical specification*, *CEN01.3: Variance control*, and *CEN01.4: Boundary location*, because they all concern the initiative system's original design. This principle also coincides with the NIST Cybersecurity Framework—specifically the 'Information Protection Processes and Procedures' category within the Protect function, whereby configuration management policies and procedures are required (Barrett, 2018). This principle also coincides with the NIST SP 800-53 Configuration Management family, as transitional organization pertains to change management (NIST Joint Task Force, 2020, p. 437).
CEN01.10: Incompletion	The principle of incompletion requires the re-initiation of the design process after evaluation and review of the current design (Cherns, 1976, p. 791). This requirement is fulfilled through the Model of Framework Use, as users are directed to evaluate the initiative using the framework between each phase of an E-Democracy initiative, as well as at the end of Gil-Garcia & Flores-Zúñiga (2020)'s implementation-adoption model of digital government success. The circular design of the model illustrates the importance of re-evaluation, as literature repeatedly shows trust and citizen engagement tend to grow over time.
CEN02: Voter DSS Requirements per Robertson (2005)	To date, no scholarly work has considered the appropriate modeling choices or theoretical approaches for using DSS as part of an E-Democracy effort to increase the policy responsiveness of governments and the civic engagement of community members. But work on DSS and electronic voting offers some relevant insights and guidelines for developing workable E-Democracy strategies. Robertson (2005) argues that, because voting is a lengthy learning and decision making process, E-Democracy efforts need to be designed as "voter support systems" that make it easier for citizens not only to vote, but also to gather and assess relevant political information so that they can select candidates who best serve their interests (p. 270). Robertson (2005) also lists seven requirements of voter DSS: (1) integration of tasks; (2) customization and personalization; (3) information gathering; (4) information retrieval and use; (5) information sharing; (6) trust, control, and information sources; and (7) diversity of users (p. 271-4). Although this research does not focus on voting electronically, the context of voting model in Robertson (2005) is like the Agawu (2017) G2C E-Democracy trends in that the first level, vote, is more of the core, basic function. As the next levels are considered, they increasingly move past basic participation and towards the creation of a nondigital equivalent, i.e., decision making, information offering, and culture and beliefs. Accordingly, this framework uses the Robertson (2005) seven DSS requirements as CEN02.x requirements for citizen engagement as a metric and uses other literature for some of the detailed elaborations of the requirements.

E-Democratic Government Success Requirements	**Description**
CEN02.1: Integration of tasks	The principle of integration of tasks requires the use of a single, integrated system that supports all current and future initiative-related tasks—accessible to users in one place for a more seamless experience (Robertson, 2005, p. 271). Porwol et al. (2013) list several types of tools government needs for e-Participation that: (a) facilitate processing of vast social media participation data; (b) interact effectively with citizens and shape discussion on deliberation platforms; (c) monitor the social media and similar place of spontaneous citizens' deliberation; (d) facilitate the processing of participation data; (e) provide feedback to citizen's contributions; (f) dissemination and reaching wide audiences; and (g) platform to invite people to participate and discuss issues (p. 291). Naicker and Mafaiti (2019) offer a model for collaboration in multisourcing information security where service providers, technology vendors, and clients share knowledge and vision through communication, coordination, and creation of formal structures for collaboration facilitated by the clients. Innovation in this requirement is demonstrated by complete integration of these tasks into one cohesive system and modeling information security multisourcing, like in Naicker & Mafaiti (2019).
CEN02.2: Customization and personalization	The principle of customization and personalization requires that users must have the ability to configure their own information filters, searches, and preferences, and to configure their own profiles (Robertson, 2005, p. 271-272). Innovation in this requirement is demonstrated by aligning customization and personalization of the initiative system with citizen needs.
CEN02.3: Information gathering	The principle of information gathering requires that users must have the ability to gather information from multiple sources in both direct and indirect ways, and that all sources of information must be easy to identify, organize, and filter by (Robertson, 2005, p. 272). Although this ability is implicitly required within the empower dynamic capability of Porwol et al. (2007)—in that facilitating the processing of vast social media participation data would inevitably include links to other sources—this principle requires the acquisition of information from multiple sources in direct and indirect ways, and the ability for users to easily search and identify sources. Separately, Nemati et al. (2002) provide the knowledge warehouse model, intended for supporting decision support systems, within which organizational decision makers are provided with an intelligent analysis platform that enhances the capturing and coding of knowledge by powering its retrieval and sharing (p. 156). Innovation in this requirement is demonstrated by using automatically generated summaries of lengthy legal texts via text mining as in Charalabidis et al. (2019), as well as conducting knowledge warehousing as in Nemati et al. (2002).

E-Democratic Government Success Requirements	**Description**
CEN02.4: Information retrieval and use	The principle of information retrieval and use requires that the initiative system must: (1) incorporate retrieval and organizational tools to help users find information when needed; (2) use existing Internet search tools and redeploy information into categories; (3) allow users to personally annotate all types of information; (4) allow users to discuss and interact about information (group annotation); and (5) allow users to associate information to issues, governmental agencies, and/or government officials (Robertson, 2005, p. 272). Porwol et al. (2013) list several types of tools government needs for e-Participation that align with these requirements, and they are tools that: (a) facilitate processing of vast social media participation data; (b) interact effectively with citizens and shape discussion on deliberation platforms; (c) monitor the social media and similar place of spontaneous citizens' deliberation; (d) facilitate the processing of participation data; (e) provide feedback to citizen's contributions; (f) dissemination and reaching wide audiences; and (g) platform to invite people to participate and discuss issues (p. 291). Naicker and Mafaiti (2019) offer a model for collaboration in multisourcing information security where service providers, technology vendors, and clients share knowledge and vision through communication, coordination, and creation of formal structures for collaboration facilitated by the clients. Innovation in this requirement is further demonstrated by the modeling of multisourcing information as in Naicker & Mafaiti (2019).
CEN02.5: Information sharing	The principle of information sharing requires that the initiative system must support communal attitude, opinion, and choice formation through the user's abilities to: (1) identify other people and groups that will help them in these activities; (2) share information easily; (3) participate and lurk in discussion groups; (4) leverage third-party browsing or searching agents for intra-initiative information; (5) send, flag, or otherwise make available information to other individuals; and (6) set sharing filters and criteria to eliminate unsolicited material (Robertson, 2005, p. 273). Porwol et al. (2013) list several types of tools government needs for e-Participation that align with these requirements, and they are tools that: (a) facilitate processing of vast social media participation data; (b) interact effectively with citizens and shape discussion on deliberation platforms; (c) monitor the social media and similar place of spontaneous citizens' deliberation; (d) facilitate the processing of participation data; (e) provide feedback to citizen's contributions; (f) dissemination and reaching wide audiences; and (g) platform to invite people to participate and discuss issues (p. 291). Nemati et al. (2002) provide the knowledge warehouse model, intended for supporting decision support systems, within which organizational decision makers are provided with an intelligent analysis platform that enhances the capturing and coding of knowledge by powering its retrieval and sharing (p. 156). Innovation in this requirement is demonstrated by conducting knowledge warehouse management as in Nemati et al. (2002).
CEN02.6: Trust, control, and information sources	The principle of trust, control, and information sources requires that the initiative system must: (1) protect user identities, participation patterns, browsing information, categorizing information, and profiling information which, where, and/or when the user defines as private; (2) only select and categorize information sources in a way that is appropriate to individual user profiles and unbiased from individual user perspectives; and (3) prohibit browsing of patterns and profiles (Robertson, 2005, p. 273). Fu et al. (2018) discuss how to combat spammers—or users that send unsolicited messages and create unsolicited social relationships through fake accounts, social bots, or spam applications—on social networks. The authors propose a dynamic metric measuring change in user activity that also quantifies users' evolution patterns which, when combined with supervised and unsupervised machine learning, has the capability of distinguishing between legitimate and illegitimate users. Separately, Charalabidis et al. (2019) describe multiple use cases of legal text mining after conducting semi-structured interviews that demonstrate the breadth of the effectiveness of DSS in different scenarios, spanning from a

E-Democratic Government Success Requirements	**Description**
	private individual to a parliamentary administrator. Innovation in this realm is demonstrated by using spam detection as in Fu et al. (2017) and text mining as in Charalabidis et al. (2019).
CEN02.7: Diversity of users	The principle of diversity of users requires that the initiative system must be accessible to the broadest swath of the jurisdiction possible, be adaptable to multiple platforms, and must not require personally owned equipment or high-end technologies to use (Robertson, 2005, p. 274). Robertson (2005) discusses the idea of outsiders (nonvoters/noncitizens) being allowed to participate in initiatives, but this is discouraged unless consented by the jurisdiction's citizens with near-unanimity due to the likelihood of negatively affecting trust in government. The diversity of users principle echoes the criteria for democratic systems given by Hansson et al. (2014), in that participants need to be equal members regardless of bureaucratic or social boundaries, and that all participants have the same status when decisions are taken. Although the success requirement *CEN01.6: Power and authority* contradicts the idea that all participants are equal members, this conflict is addressed by the democratic election of those in higher power/authority than typical users.
Security (SEC)	E-Government projects not only need to enhance democratic responsiveness and engagement, but they also need to guarantee the privacy of users and ensure digital systems are reliable and secure. This framework assesses security through three perspectives: risk management, cybersecurity maturity, and disinformation prevention. Although only risk management and cybersecurity are related, disinformation prevention relates to each of the CEN02 requirements, and all three are related with all TGV requirements and various CEN01 requirements. Gerber & von Somms (2008) propose a model for determining organizations' legal requirements, and in doing so, demonstrate how inadequate the laws and regulations are when compared to a comprehensive security framework like ISO/IEC 27002 or the NIST Special Publication (SP) 800 series. Accordingly, this guidance refers to multiple external security standards, frameworks, and models— such as the McCumber Cube (McCumber, 2004), NIST Special Publication (SP) 800-37 (NIST Joint Task Force, 2018), NIST SP 800-53 (NIST Joint Task Force, 2020), and the NIST Cybersecurity Framework (Barrett, 2018)— rather than only regulatory statutes.

E-Democratic Government Success Requirements	**Description**
SEC01: Risk Management	NIST Special Publication (SP) 800-37 is a risk management framework that functions as a system life cycle for security and privacy risk assessment, and centers around a risk management process consisting of seven steps: (1) prepare, in which emphasis is placed on the importance of organization-wide governance and risk management through ongoing activities; (2) categorize, in which risk management processes and tasks are informed by assessing potential impact to affected parties in terms of confidentiality, integrity, and availability of systems and information processed, stored, and transmitted by those systems; (3) select, in which necessary controls are selected, tailored, and documented to protect against risk to affected parties; (4) implement, in which controls are implemented and baseline configuration and specific details of implementation are documented; (5) assess, in which controls selected for implementation are assessed to determine if they were implemented, operating, and producing the desired outcome correctly; (6) authorize, in which a senior management official is required to determine and stand accountable for whether security and privacy risk to affected parties, assets, and systems is acceptable; and (7) monitor, in which an ongoing situational awareness about security and privacy posture is maintained (NIST Joint Task Force, 2018, p. 23-83). NIST SP 800-53 specifies hundreds of controls for security and privacy for federal information systems across the following twenty categories, called families: access control (AC); awareness and training (AT); audit and accountability (AU); assessment, authorization, and monitoring (CA); configuration management (CM); contingency planning (CP); identification and authentication (IA); incident response (IR); maintenance (MA); media protection (MP); physical and environmental protection (PE); planning (PL); program management (PM); personnel security (PS); personally identifiable information processing and transparency (PT); risk assessment (RA); system and services acquisition (SA); system and communications protection (SC); system and information integrity (SI); and supply chain risk management (SR) (NIST Joint Task Force, 2020). These NIST SP 800-53 controls must be individually and continually assessed using the NIST SP 800-37 risk management process at least once before the adoption stage of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), and once annually or as change occurs. Completion of this process inherently satisfies NIST SP 800-53 control RA-3(a), Conduct a Risk Assessment. Innovation in this realm is demonstrated by conducting complete risk assessments more often, determining gaps between this process and emerging risks to the initiative, and adapting the risk management process to incorporate newly discovered risks that are unaddressed in NIST SP 800-37 and/or NIST SP 800-53 using other relevant frameworks or publications. For example, Lidén (2013) identifies numerous constructs affecting the supply and demand of E-Democracy services in Sweden, such as the technological divide between who was and was not likely to use E-Democracy services. Although these newly discovered constructs are not incorporated into a risk management process within this work, the McCumber (2004) Cube model or the NICE Framework (NIST SP 800-181, Petersen et al., 2020) could be used to assist such incorporation.
SEC02: Cybersecurity Maturity	Assessment of cybersecurity maturity must be incorporated into the framework, as research has consistently demonstrated the importance of maturity in the longevity of technological products and organizations. For example, Fraser & Vaishnavi (1997) propose a measurement model for capability maturity levels of formal specification processes in software development environments which proved impactful in positively affecting this area of research. This framework considers E-Democracy initiatives as critical infrastructure, as their eventual criticality is unknown—although likely to become perceived as critical with time. Because the target audience includes any U.S. jurisdiction, the NIST Cybersecurity Framework— consisting of five categories: identify, protect, detect, respond, and recover— is best suited as an evaluation tool for cybersecurity maturity in this case (Barrett, 2018; Miron & Muita, 2014). Thus, full compliance with the

E-Democratic Government Success Requirements	**Description**
	NIST Cybersecurity Framework is required for the baseline standard. Each NIST Cybersecurity Framework subcategory maps to NIST SP 800-53 controls (NIST Joint Task Force, 2020); accordingly, SEC01 reinforces the baseline standard of this requirement. Although this framework uses Defense in Depth strategy (U.S. National Security Agency, 2015) through demonstrating the interrelated nature of the requirements, innovation in this requirement is demonstrated by the further application, measurement, and evaluation of Defense in Depth strategy into the initiative. For example, Groat et al. (2012) proposed symmetric (zero-trust) Defense in Depth to prevent both intrusion and data exfiltration, as well as systematic dynamic defenses which keep attack surfaces constantly changing in network information to prevent attacks. Although more research is needed in this area, other examples of applying Defense in Depth strategy to industrial control systems are given in Mell et al. (2016) and U.S. Department of Homeland Security (2016).
SEC03: Disinformation Prevention	Farrell & Schneier (2018) suggest we should view democracies and other forms of government as information systems, and information through the lens of common versus contested knowledge, in that common knowledge is what needs to be shared for the political system to function, and contested knowledge is with what people may disagree (p. 6). Critically, the authors note that, if political institution common knowledge (election results, succession of power) and/or the range of actors, beliefs, and opinions in a society fall from common knowledge to contested knowledge, the system can no longer function (Farrell & Schneier, 2018, p. 8-9). Accordingly, the lines between common and contested knowledge must be clearly defined and accepted amongst a community for an E-Democracy initiative to exist and persist. Compliance with this requirement is met through the identification and labeling of information as accepted as truth, deemed false, or undetermined/questionable—and identifications and labels must be agreed to by a minimum of a simple majority of users to prevent catastrophic failure in keeping with democratic principles as described by Farrell & Schneier (2018). Innovation in this realm is demonstrated through higher levels of agreement in identification and labeling of information, as well as robust, semi-automated identification and labeling of information using a combination of machine learning (like how Tesfay et al. (2018) use machine learning to automatically determine grades of eleven different privacy aspects in a supplied privacy policy) and transparent human review of initiative information via the democratic election of a group of users.
Privacy (PRV) per Gerber et al. (2018)	Any E-Democratic Government platform must recognize that, while most users have an interest in maintaining their privacy, they tend to have a poor track record in doing so. One problem for users is that privacy—a notoriously difficult concept to define—can pertain to physical seclusion, informational secrecy, and informational control depending on the context. Users are not necessarily making these distinctions or keeping them constantly in mind. Smith et al. (2011) specifies that information privacy, and not physical privacy, is within the scope of what most cyber or information systems research today would call privacy in this realm. The authors then further categorize what privacy is: (1) a value-based right, (2) a value-based commodity, (3) a cognate-based state, and (4) a cognate-based control—and what it is not: (1) anonymity, (2) secrecy, (3) confidentiality, (4) security, and (5) ethics (Smith et al., 2011, p. 994-7). Although the authors clarify that the value-based definitions should not be treated absolutely, as they often conflict with legal and societal frameworks, they also specify that privacy has a contextual nature. Although SEC01 also requires use of NIST SP 800-53, SEC01 addresses the cognate-based control definition and not the other three (NIST Joint Task Force, 2020). As value-based rights to privacy are addressed through the CEN requirements, this requirement focuses on the value-based commodity and cognate-based state definitions of privacy. Separately, Gerber et al. (2018) discuss the privacy paradox: a privacy phenomenon where users often indicate one privacy preference when surveyed yet behave in ways that contradict their survey answers. It remains unclear what drives this paradox, but Gerber et al.

E-Democratic Government Success Requirements	**Description**
	(2018) find that the privacy paradox is likely driven by a combination of cognitive biases that push users to underestimate costs from privacy losses, especially over the long term. Specifically, the authors identify four categories of predictor variables for future studies: (1) privacy attitude, concerns, and perceived risk; (2) privacy related behavioral intention and willingness; (3) information disclosure behavior; and (4) protection behavior and privacy settings (p. 249-251). Accordingly, these categories are used to inform this requirement's subcategories, and developers need to make privacy safeguards easy to use and understand—perhaps by setting strong privacy settings as default. As an example of ideal communication of privacy, *PrivacyGuide* by Tesfay et al. (2018) accepts URLs leading to companies' privacy policies and provide letter grades on eleven different privacy aspects (data collection, protection of children, third-party sharing, data security, data retention, data aggregation, control of data, privacy settings, account deletion, privacy breach notification, and policy changes) using the open-source machine learning tool, *WEKA* (p. 19). Innovation in this realm is demonstrated by the use of text summarization using machine learning to automatically inform initiative management of user privacy.
PRV01: Privacy attitude, concerns, and perceived risk	This requirement is concerned with what Smith et al. (2011) would consider the cognate-based state, consisting of three categories: privacy attitudes, privacy concerns, and perceived privacy risk (Gerber et al., 2018, p. 246). The first category, privacy attitudes, informs the following outcome variables: attitude towards location-based mobile websites, attitude towards information practice, attitude towards location based social network apps, attitude towards social network games, social scientists' attitude towards data sharing, and general attitude towards privacy. The second category, privacy concerns, informs outcome variables measuring general privacy concern, website privacy controls, context specific privacy concerns, and health information privacy concern. The last category, perceived privacy risk, is its own outcome variable. Predictor variables for this requirement include trust, informational privacy concerns, computer anxiety, perceived privacy risk, permission granted, perceived control, consumer alienation, self-esteem, interaction with IT, data transfer internally, perceived security, perceived benefit, perceived playfulness, website reputation, disposition to privacy, perceived career benefit, level of trust in the recipient's ability to protect data, personalization, perceived relevance of information, perceived health information sensitivity, perceived privacy regulatory protection, and privacy risk awareness (Gerber et al., 2018, p. 246).
PRV02: Privacy-related behavioral intention and willingness	This requirement blends between the Smith et al. (2011) cognate-based state definition of privacy and the value-based commodity definition of privacy. Per Gerber et al. (2018), the benefits gained through data disclosure are important predictors of behavioral intention and willingness to disclose data. However, the constructs measuring need for consent and the degree to which a user considers the transaction a typical case of data disclosure were found to be stronger predictors of intention and willingness to disclose data (Gerber et al., 2018, p. 248-249). Outcome variables include general intention to disclose information, willingness to disclose information, intention to make Facebook data publicly available, intention to disclose information on social networking sites, intention to disclose data to an online retailer, and willingness to disclose information about peer relationships on Facebook. Predictor variables include website trust, perceived benefit/value, liked targeted ads, need for consent, retention period, collection concerns, website privacy concern, perceived privacy risk, privacy concern, willingness, perceived usefulness, usage scope, attitude, prototype similarity, and privacy protection belief (Gerber et al., 2018, p. 246).

E-Democratic Government Success Requirements	Description
PRV03: Information disclosure behavior	This requirement blends between the Smith et al. (2011) cognate-based state definition of privacy and the value-based commodity definition of privacy. Information disclosure behavior was found to be strongly predicted by intention to disclose and general willingness to self-disclose (Gerber et al., 2018, p. 248-249). Outcome variables include information disclosure on social networking sites, teen information disclosure on social media, usage of social network games, general information disclosure, disclosure towards a mobile app recommender, and location disclosure on location based-social network application. Predictor variables include privacy intention, general willingness to self-disclose, collection concerns, attitude towards location-based social network application, privacy concerns, number of applications, entertainment benefits, basic information disclosure, ads awareness, social relevance, gender, and mobile internet usage (Gerber et al. 2018, p. 247).
PRV04: Protection behavior and privacy settings	This requirement blends between the Smith et al. (2011) cognate-based state definition of privacy and the value-based commodity definition of privacy. Users' protective data behaviors were found to be best predicted by their participation in risky interactions and behavioral intention (Gerber et al., 2018, p. 248-249). Outcome variables include teenage privacy protection on social networking sites, privacy settings on social networking sites, and privacy-protective behaviors. Predictor variables include risky interaction, intention, privacy risk concerns, perceived norms regarding what to show only to friends, and years of internet experience (Gerber et al. 2018, p. 247).

PART THREE — STANDARDS, RELATIONSHIPS, AND LITERATURE

Table 4.2. Standards of e-democratic government success requirements

E-Democratic Government Success Requirements	**Baseline**	**Intermediate**	**Innovative**
E-Government Trends per Agawu (2017)	One or more of the E-Democracy trends by Agawu (2017)—increasing access to relevant information and content, digitizing the service loop, and/or creating/expanding government function—are meaningfully present within the initiative.	Two or more of the E-Democracy trends by Agawu (2017)—increasing access to relevant information and content, digitizing the service loop, and/or creating/expanding government function—are meaningfully present within the initiative.	All three of the E-Democracy trends by Agawu (2017)—increasing access to relevant information and content, digitizing the service loop, and/or creating/expanding government function—are meaningfully present within the initiative.
Trust In Government (TGV) per Papp et al. (2020)			
TGV01: Behavioral trust	Citizens' trust in government sentiments regarding government officials' personal characteristics are collected, measured, analyzed, evaluated, and interpreted through tedious means, i.e., surveys, town hall meetings, etc. Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a simple majority or greater of citizens' expressed sentiments. Requires skills in data collection and analysis; ability to navigate, understand, and adapt government and its officials; ability to understand and appropriately respond to citizens' expressed sentiments of government officials.	Citizens' trust in government sentiments regarding government officials' personal characteristics are collected, measured, analyzed, evaluated, and interpreted using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Requires conducting predictive data analysis to experiment with predicting citizen trust in government sentiments against government officials' personal characteristics reliably. Requires knowledge of external conditions (political, social, and economical) and maintaining/increasing trust in government from a two-thirds majority or greater of citizens' expressed sentiments. Requires skills in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al.,	Citizens' trust in government sentiments regarding government officials' personal characteristics are collected, measured, analyzed, evaluated, and interpreted using technologies that have a nondigital equivalent, e.g., text mining social media posts, knowledge management solutions that greatly enhance the functionality of data (Kulkarni et al., 2006; Nemati et al., 2002), a platform specifically tailored to the purpose of trust in government sentiment analysis, etc. Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a three-quarters majority or greater of citizens' expressed sentiments. Requires skills and innovation in responsive design and reputational systems for technological

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
		2019); digital data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, appropriately respond to, and tentatively predict citizens' expressed sentiments of government officials.	initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, communicate with, appropriately respond to, and ethically and reliably predict citizens' expressed sentiments of government officials.
TGV01.1: Tasks	Citizens' trust in government sentiments regarding government officials' personal characteristics are collected, measured, analyzed, evaluated, and interpreted through tedious means, i.e., surveys, town hall meetings, etc.	Citizens' trust in government sentiments regarding government officials' personal characteristics are collected, measured, analyzed, evaluated, and interpreted using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Requires conducting predictive data analysis to experiment with predicting citizen trust in government sentiments against government officials' personal characteristics until prediction is reliable.	Citizens' trust in government sentiments regarding government officials' personal characteristics are collected, measured, analyzed, evaluated, and interpreted using technologies that have a nondigital equivalent, e.g., text mining social media posts, knowledge management solutions that greatly enhance the functionality of data (Kulkarni et al., 2006; Nemati et al., 2002), a platform specifically tailored to the purpose of trust in government sentiment analysis, etc.
TGV01.2: Knowledge	Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a simple majority or greater of citizens' expressed sentiments.	Requires knowledge of external conditions (political, social, and economical) and maintaining/increasing trust in government from a two-thirds majority or greater of citizens' expressed sentiments.	Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a three-quarters majority or greater of citizens' expressed sentiments.
TGV01.3: Skills	Requires skills in data collection and analysis; ability to navigate, understand, and adapt government and its officials; ability to understand and appropriately respond to citizens' expressed sentiments of government officials.	Requires skills in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to	Requires skills and innovation in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
		understand, appropriately respond to, and tentatively predict citizens' expressed sentiments of government officials.	technology; ability to understand, communicate with, appropriately respond to, and ethically and reliably predict citizens' expressed sentiments of government officials.
TGV02: Operational trust	Citizens' trust in government sentiments regarding government processes are collected, measured, analyzed, evaluated, and interpreted through tedious means, i.e., surveys, town hall meetings, etc. Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a simple majority or greater of citizens' expressed sentiments. Requires skills in data collection and analysis; ability to navigate, understand, and adapt government and its officials; ability to understand and appropriately respond to citizens' expressed sentiments of government processes.	Citizens' trust in government sentiments regarding government processes are collected, measured, analyzed, evaluated, and interpreted using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Conduct predictive data analysis to experiment with predicting citizen trust in government sentiments against government processes until prediction is reliable. Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a two-thirds majority of citizens' expressed sentiments; responsive design in technological initiatives (Germonprez et al., 2017). Requires skills in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, appropriately respond to, and tentatively predict citizens' expressed sentiments of government processes.	Citizens' trust in government sentiments regarding government processes are collected, measured, analyzed, evaluated, interpreted, and predicted using technologies that have a nondigital equivalent, i.e., text mining social media posts, knowledge management solutions that greatly enhance the functionality of data (Kulkarni et al., 2006; Nemati et al., 2002), a platform specifically tailored to the purpose of trust in government sentiment analysis, etc. Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a three-quarters majority of citizens' expressed sentiments; responsive design in both technological initiatives and government (Germonprez et al., 2017); the ethical and moral implications surrounding the prediction of citizen trust in government sentiments. Requires skills and innovation in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
			adapt government, its officials, and its technology; ability to understand, communicate with, appropriately respond to, and ethically and reliably predict citizens' expressed sentiments of government processes.
TGV02.1: Tasks	Citizens' trust in government sentiments regarding government processes are collected, measured, analyzed, evaluated, and interpreted through tedious means, i.e., surveys, town hall meetings, etc.	Citizens' trust in government sentiments regarding government processes are collected, measured, analyzed, evaluated, and interpreted using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Conduct predictive data analysis to experiment with predicting citizen trust in government sentiments against government processes until prediction is reliable.	Citizens' trust in government sentiments regarding government processes are collected, measured, analyzed, evaluated, interpreted, and predicted using technologies that have a nondigital equivalent, i.e., text mining social media posts, knowledge management solutions that greatly enhance the functionality of data (Kulkarni et al., 2006; Nemati et al., 2002), a platform specifically tailored to the purpose of trust in government sentiment analysis, etc.
TGV02.2: Knowledge	Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a simple majority or greater of citizens' expressed sentiments.	Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a two-thirds majority of citizens' expressed sentiments; responsive design in technological initiatives (Germonprez et al., 2017).	Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a three-quarters majority of citizens' expressed sentiments; responsive design in both technological initiatives and government (Germonprez et al., 2017); the ethical and moral implications surrounding the prediction of citizen trust in government sentiments.
TGV02.3: Skills	Requires skills in data collection and analysis; ability to navigate, understand, and adapt government and its officials; ability to understand and appropriately	Requires skills in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection,	Requires skills and innovation in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
	respond to citizens' expressed sentiments of government processes.	analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, appropriately respond to, and tentatively predict citizens' expressed sentiments of government processes.	collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, communicate with, appropriately respond to, and ethically and reliably predict citizens' expressed sentiments of government processes.
TGV03: Institutional trust	Citizens' trust in government sentiments regarding actions, policies, and/or regulations of governmental institutions and/or their agents are collected, measured, analyzed, evaluated, and interpreted through tedious means, i.e., surveys, town hall meetings, etc. Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a simple majority or greater of citizens' expressed sentiments. Requires skills in data collection and analysis; ability to navigate, understand, and adapt government and its officials; ability to understand and appropriately respond to citizens' expressed sentiments of governmental institutions and/or their agents.	Citizens' trust in government sentiments regarding actions, policies, and/or regulations of governmental institutions and/or their agents are collected, measured, analyzed, evaluated, and interpreted using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Conduct predictive data analysis to experiment with predicting citizen trust in government sentiments against government institutions and/or their agents until prediction is reliable. Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a two-thirds majority of citizens' expressed sentiments; responsive design in technological initiatives (Germonprez et al., 2017). Requires skills in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its	Citizens' trust in government sentiments regarding actions, policies, and/or regulations of governmental institutions and/or their agents are collected, measured, analyzed, evaluated, interpreted, and predicted using technologies that have a nondigital equivalent, i.e., text mining social media posts, knowledge management solutions that greatly enhance the functionality of data (Kulkarni et al., 2006; Nemati et al., 2002), a platform specifically tailored to the purpose of trust in government sentiment analysis, etc. Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a three-quarters majority of citizens' expressed sentiments; responsive design in both technological initiatives and government (Germonprez et al., 2017); the ethical and moral implications surrounding the prediction of citizen trust in government sentiments. Requires skills and innovation in responsive design and reputational

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
		officials, and its technology; ability to understand, appropriately respond to, and tentatively predict citizens' expressed sentiments of governmental institutions and/or their agents.	systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, communicate with, appropriately respond to, and ethically and reliably predict citizens' expressed sentiments of governmental institutions and/or their agents.
TGV03.1: Tasks	Citizens' trust in government sentiments regarding actions, policies, and/or regulations of governmental institutions and/or their agents are collected, measured, analyzed, evaluated, and interpreted through tedious means, i.e., surveys, town hall meetings, etc.	Citizens' trust in government sentiments regarding actions, policies, and/or regulations of governmental institutions and/or their agents are collected, measured, analyzed, evaluated, and interpreted using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Conduct predictive data analysis to experiment with predicting citizen trust in government sentiments against government institutions and/or their agents until prediction is reliable.	Citizens' trust in government sentiments regarding actions, policies, and/or regulations of governmental institutions and/or their agents are collected, measured, analyzed, evaluated, interpreted, and predicted using technologies that have a nondigital equivalent, i.e., text mining social media posts, knowledge management solutions that greatly enhance the functionality of data (Kulkarni et al., 2006; Nemati et al., 2002), a platform specifically tailored to the purpose of trust in government sentiment analysis, etc.
TGV03.2: Knowledge	Requires knowledge of external conditions (political, social, and economic) and maintaining/increasing trust in government from a simple majority or greater of citizens' expressed sentiments.	Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a two-thirds majority of citizens' expressed sentiments; responsive design in technological initiatives (Germonprez et al., 2017).	Requires knowledge of external conditions (previous experiences, political, social, and economic); maintaining/increasing trust in government from no less than a three-quarters majority of citizens' expressed sentiments; responsive design in both technological initiatives and government (Germonprez et al., 2017); the ethical and moral implications surrounding the

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
			prediction of citizen trust in government sentiments.
TGV03.3: Skills	Requires skills in data collection and analysis; ability to navigate, understand, and adapt government and its officials; ability to understand and appropriately respond to citizens' expressed sentiments of governmental institutions and/or their agents.	Requires skills in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, appropriately respond to, and tentatively predict citizens' expressed sentiments of governmental institutions and/or their agents.	Requires skills and innovation in responsive design and reputational systems for technological initiatives (Germonprez et al., 2017; Hanson et al., 2019); data collection, analysis, and science; ability to navigate, understand, and adapt government, its officials, and its technology; ability to understand, communicate with, appropriately respond to, and ethically and reliably predict citizens' expressed sentiments of governmental institutions and/or their agents.
Citizen Engagement (CEN)			
CEN01: Design using STT per Cherns (1987)	Initiative must meet at least the baseline standard of each of the CEN01 requirements.	Initiative must meet at least the intermediate standard of each of the CEN01 requirements.	Initiative must meet at least the innovative standard of each of the CEN01 requirements.
CEN01.1: Compatibility	Design process of initiative must be compatible with digitization of one or more of the following policymaking stages, and such digitization has been completed or meaningfully initiated: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and (5) monitoring the policy (Grönlund, 2003).	Design process of initiative must be compatible with digitization of three or more of the following policymaking stages, and such digitization has been completed: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and (5) monitoring the policy (Grönlund, 2003). Knowledge management systems, architecture, and/or methods support at least one of these digitized policymaking stages (Mergel, 2010; Nemati et al. 2002; Porwol et al. 2013).	Design process of initiative must be compatible with digitization of all five of the following policymaking stages, and such digitization has been completed: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and (5) monitoring the policy (Grönlund, 2003). Knowledge management systems, architecture, and/or methods support at least three of these digitized policymaking stages (Mergel, 2010; Nemati et al. 2002; Porwol et al. 2013).

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
CEN01.2: Minimal critical specification	Tasks, jobs, and roles of the initiative must be clearly defined, and mapping of connections between those tasks, jobs, and roles must be completed according to the NICE Framework (NIST SP 800-181; Petersen et al., 2020) to demonstrate that no one task, job, or role specifies no more and no less than the following essential tasks: citizens' sentiments are collected, measured, analyzed, evaluated, interpreted, and reasonably addressed by government, government acknowledges citizen contributions with feedback and simultaneously requests citizen participation.	Tasks, jobs, and roles of the initiative must be clearly defined, and mapping of connections between those tasks, jobs, and roles must be completed according to the NICE Framework (NIST SP 800-181; Petersen et al., 2020) to demonstrate that no one task, job, or role specifies no more and no less than the following essential tasks: citizens' sentiments are collected, measured, analyzed, evaluated, and interpreted by government; government acknowledges citizen contributions with feedback, simultaneously requests citizen participation; and both government and citizens simultaneously empower each other (Porwol et al., 2013).	Tasks, jobs, and roles of the initiative must be clearly defined, and mapping of connections between those tasks, jobs, and roles must be completed according to the NICE Framework (NIST SP 800-181; Petersen et al., 2020) to demonstrate that no one task, job, or role specifies no more and no less than the following essential tasks: citizens' sentiments are collected, measured, analyzed, evaluated, interpreted, and predicted by government; government acknowledges citizen contributions with feedback; government stimulates digital participation using tools for dissemination to reach wide audiences while simultaneously requesting citizen participation; and both government and citizens simultaneously empower each other (Porwol et al., 2013).
CEN01.3: Variance control	All participants of the initiative must be equal members (aside from elected power users, see *CEN01.6: Power and authority*) and have the same status when decisions are taken, requiring that no social or bureaucratic boundaries are reflected in user accounts.	All participants of the initiative must be equal members (aside from elected power users, see *CEN01.6: Power and authority*) and have the same status when decisions are taken, requiring that no social or bureaucratic boundaries are reflected in user accounts. Aggregated public user contribution and outcome data must be available to users and presented in a way that satisfies privacy expectations of the user base.	All participants of the initiative must be equal members (aside from elected power users, see *CEN01.6: Power and authority*) and have the same status when decisions are taken, requiring that no social or bureaucratic boundaries are reflected in user accounts. Individual and aggregated public user contribution and outcome data must be available to users and presented in a way that satisfies privacy expectations of the user base.
CEN01.4: Boundary location	Initiative boundaries must be drawn to facilitate—and not hinder—the sharing of information, knowledge, and/or learning.	Initiative boundaries must be drawn to facilitate—and not hinder—the sharing of information, knowledge, and/or learning.	Initiative boundaries must be drawn to facilitate to the degree possible, and not hinder, the sharing of information,

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
		Modeling and evaluation of community commitment and information multisourcing must have been completed at least once (Bateman et al., 2011; Naicker & Mafaiti, 2019).	knowledge, and/or learning. Modeling and evaluation of community commitment and multisourcing must be completed at least once annually (Bateman et al., 2011; Naicker & Mafaiti, 2019).
CEN01.5: Information flow	All initiative participants must be provided with relevant information during system design and engineering activities, organizational change processes, and when they otherwise require it. Information flow is modeled and mapped to these activities (Baxter & Sommerville, 2011; Porwol et al., 2013).	All initiative participants must be provided with relevant information during system design and engineering activities, organizational change processes, and when they otherwise require it. Information flow is modeled and mapped to these activities, and aggregated information flow data are transparently available to users and presented in a way that maintains privacy expectations of the user base (Baxter & Sommerville, 2011; Porwol et al., 2013; Antoni et al., 2017).	All initiative participants must be provided with relevant information during system design and engineering activities, organizational change processes, and when they otherwise require it. Information flow is modeled and mapped to these activities, and individual and aggregated information flow data are transparently available to users and presented in a way that maintains privacy expectations of the user base (Baxter & Sommerville, 2011; Porwol et al., 2013; Antoni et al., 2017).
CEN01.6: Power and authority	Participants of the initiative must democratically elect one or more individuals to short-term power roles that grant wider access to resources than typical users receive, and those individuals must not only have access to required resources according to their responsibilities, but also must accept responsibility for the prudent and economical use of those resources—including accepting prohibition from using the platform as other users would. Users must have the ability to revoke the individuals' wider access or otherwise recall them with a majority vote.	Participants of the initiative must democratically elect one or more individuals to short-term power roles that grant wider access to resources than typical users receive, and those individuals must not only have access to required resources according to their responsibilities, but also must accept responsibility for the prudent and economical use of those resources—including accepting prohibition from using the platform as other users would. Users must have the ability to revoke the individuals' wider access or otherwise recall them with a majority vote. Aggregated power user data is	Participants of the initiative must democratically elect one or more individuals to short-term power roles that grant wider access to resources than typical users receive, and those individuals must not only have access to required resources according to their responsibilities, but also must accept responsibility for the prudent and economical use of those resources—including accepting prohibition from using the platform as other users would. Users must have the ability to revoke the individuals' wider access or otherwise recall them with a majority vote. Individual and aggregated power user data is

E-Democratic Government Success Requirements	**Baseline**	**Intermediate**	**Innovative**
		transparently available to standard users (Antoni et al., 2017).	transparently available to standard users (Antoni et al., 2017).
CEN01.7: Multifunctionality	The initiative must give the ability to add new roles and modify existing roles to those who manage the initiative. Qualitative gap analysis between existing roles and organizational, governmental, and constituent needs must be conducted at least once annually.	The initiative must give the ability to add new roles and modify existing roles to those who manage the initiative. Users must be able to guide the addition or modification of roles through engagement with the initiative but may not be able to directly do so. Qualitative gap analysis between existing roles and organizational, governmental, and constituent needs must be conducted at least once annually.	The initiative must give users the ability to add new roles and modify existing roles. Qualitative gap analysis between existing roles and organizational, governmental, and constituent needs must be conducted at least once annually.
CEN01.8: Support congruence	Qualitative gap analysis on the initiative's support systems, support roles, support functions, and one or more of the following policymaking stages must be conducted at least once every three years: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and (5) monitoring the policy (Grönlund, 2003). This standard also requires that support systems, roles, and/or functions that are determined not to support one or more of these stages be decommissioned, retired, and/or removed from the initiative.	Qualitative gap analysis on the initiative's support systems, support roles, support functions, and three or more of the following policymaking stages must be conducted at least once every three years, and as new support systems, roles, and/or functions are added: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and (5) monitoring the policy (Grönlund, 2003). This standard also requires that support systems, roles, and/or functions that are determined not to support one or more of these stages directly or indirectly be decommissioned, retired, and/or removed from the initiative.	Qualitative gap analysis on the initiative's support systems, support roles, support functions, and all five of the following policymaking stages must be conducted once annually, and as new support systems, roles, and/or functions are added: (1) agenda setting, (2) analysis, (3) creating the policy, (4) implementing the policy, and (5) monitoring the policy (Grönlund, 2003). This standard also requires that support systems, roles, and/or functions that are determined not to support one or more of these stages directly or indirectly be decommissioned, retired, and/or removed from the initiative.
CEN01.9: Transitional organization	All initiative transitions and changes must be planned and designed by those who manage the initiative before they occur. Qualitative gap analysis between existing roles and organizational, governmental,	All initiative transitions and changes must be planned and designed by those who manage the initiative before they occur, and the users must approve of the changes before they are implemented. Qualitative	All initiative transitions and changes must be planned, designed, and approved by the users before they occur. Qualitative gap analysis between existing roles and organizational, governmental, and

E-Democratic Government Success Requirements	**Baseline**	**Intermediate**	**Innovative**
	and constituent needs must be conducted at least once annually.	gap analysis between existing roles and organizational, governmental, and constituent needs must be conducted at least once annually.	constituent needs must be conducted at least once annually.
CEN01.10: Incompletion	Evaluation using this framework must be completed between each phase of E-Democracy initiatives shown in the Model of Framework Use (Figure 3.1), and at least once after each iteration of the demand phase of the initiative.	Evaluation using this framework must be completed between each phase of E-Democracy initiatives shown in the Model of Framework Use (Figure 3.1), at least once after each iteration of the demand phase of the initiative, and annually at minimum.	Evaluation using this framework must be completed between each phase of E-Democracy initiatives shown in the Model of Framework Use (Figure 3.1), and at least once after each iteration of the demand phase of the initiative, and bi-annually at minimum.
CEN02: Voter DSS Requirements per Robertson (2005)	Initiative must meet at least the baseline standard of each of the CEN02 requirements.	Initiative must meet at least the intermediate standard of each of the CEN02 requirements.	Initiative must meet at least the innovative standard of each of the CEN02 requirements.
CEN02.1: Integration of tasks	Each of the Porwol et al. (2013) tools that government needs for e-Participation must be present within the initiative within one cohesive system, and each adheres to the adaptive standard of dynamic capabilities given in that work.	Each of the Porwol et al. (2013) tools that government needs for e-Participation must be present within the initiative within one cohesive system, and each adheres to at least the absorptive standard of dynamic capabilities given by the author. Modeling and evaluation of information multisourcing must have been completed at least once (Naicker & Mafaiti, 2019).	Each of the Porwol et al. (2013) tools that government needs for e-Participation must be present within the initiative within one cohesive system, and each adheres to at least the innovative standard of dynamic capabilities given by the author. Modeling and evaluation of information multisourcing is completed at least once annually (Naicker & Mafaiti, 2019).
CEN02.2: Customization and personalization	Users must have the ability to configure their own information filters, searches, preferences, and profiles within any initiative system.	Users must have the ability to configure their own information filters, searches, preferences, and profiles within any initiative system. Updates to initiative system(s) are conducted periodically to address citizen information needs.	Users must have the ability to configure their own information filters, searches, preferences, and profiles within any initiative system. Users can freely construct their own solutions to emerging information needs.
CEN02.3: Information gathering	Users must have the ability to gather information, both directly and indirectly, from multiple sources. Sources of	Users must have the ability to gather information, both directly and indirectly, from multiple sources. Sources of information gathered by users must be	Users must have the ability to gather information, both directly and indirectly, from multiple sources. Sources of information gathered by users must be

E-Democratic Government Success Requirements	**Baseline**	**Intermediate**	**Innovative**
	information gathered by users must be easily identified, organized, and filtered.	easily identified, organized, and filtered. Knowledge warehouse systems must be used to facilitate citizen learning and decision support, as in Nemati et al. (2002).	easily identified, organized, and filtered. Knowledge warehouse systems must be used to facilitate citizen learning and decision support, as in Nemati et al. (2002). Unbiased summaries of lengthy legal texts must be provided through text mining (Charalabidis et al, 2019).
CEN02.4: Information retrieval and use	Users must have the ability to use retrieval and organizational tools within the initiative system; use search tools external to the initiative system for initiative information; redeploy information into categories; annotate all types of information; discuss and interact with other users about information; and associate information to issues, governmental agencies, and government officials.	Users must have the ability to use retrieval and organizational tools within the initiative system; use search tools external to the initiative system for initiative information; redeploy information into categories; annotate all types of information; discuss and interact with other users about information; and associate information to issues, governmental agencies, and government officials. Modeling and evaluation of information multisourcing has been completed at least once (Naicker & Mafaiti, 2019).	Users must have the ability to use retrieval and organizational tools within the initiative system; use search tools external to the initiative system for initiative information; redeploy information into categories; annotate all types of information; discuss and interact with other users about information; and associate information to issues, governmental agencies, and government officials. Modeling and evaluation of information multisourcing is completed at least once annually (Naicker & Mafaiti, 2019).
CEN02.5: Information sharing	Users must have the ability to identify people and groups that will assist in attitude, opinion, and choice formation; share information easily; participate and lurk in discussion groups; use third-party browsing or searching agents for intra-initiative information; send, flag, or otherwise make available information to other individuals; and set sharing filters and criteria to eliminate unsolicited material.	Users must have the ability to identify people and groups that will assist in attitude, opinion, and choice formation; share information easily; participate and lurk in discussion groups; use third-party browsing or searching agents for intra-initiative information; send, flag, or otherwise make available information to other individuals; and set sharing filters and criteria to eliminate unsolicited material. Knowledge warehouse systems must be used to facilitate information sharing, as in Nemati et al. (2002).	Users must have the ability to identify people and groups that will assist in attitude, opinion, and choice formation; share information easily; participate and lurk in discussion groups; use third-party browsing or searching agents for intra-initiative information; send, flag, or otherwise make available information to other individuals; and set sharing filters and criteria to eliminate unsolicited material. Knowledge warehouse systems must be optimized and used to facilitate information sharing, as in Nemati et al. (2002).

E-Democratic Government Success Requirements	**Baseline**	**Intermediate**	**Innovative**
CEN02.6: Trust, control, and information sources	Users must have the ability to define their identities, participation patterns, browsing information, categorizing information, and profiling information as private; select and categorize information sources only in a way that is appropriate to individual user profiles and unbiased from individual user perspectives; and prohibit browsing of their patterns and profiles.	Users must have the ability to define their identities, participation patterns, browsing information, categorizing information, and profiling information as private; select and categorize information sources only in a way that is appropriate to individual user profiles and unbiased from individual user perspectives; and prohibit browsing of their patterns and profiles. Spam and spammers are manually identified by means mutually agreed upon by government and citizens, and their accounts, profiles, and/or contributions to the platform are removed once identified. The use of text mining to expedite manual review, like in Charalabidis et al. (2019), is recommended.	Users must have the ability to define their identities, participation patterns, browsing information, categorizing information, and profiling information as private; select and categorize information sources only in a way that is appropriate to individual user profiles and unbiased from individual user perspectives; and prohibit browsing of their patterns and profiles. Spam and spammers are identified automatically by algorithms, as in Fu et al. (2017), and their accounts, profiles, and/or contributions to the platform are removed once manually verified as spam/spammer. The use of text mining to expedite manual review, like in Charalabidis et al. (2019), is required.
CEN02.7: Diversity of users	Any initiative system must be accessible to the broadest swath of the target jurisdiction possible; allow, invite, and proactively recruit legitimate users to the initiative; and be accessible from multiple platforms, operating systems, browsers, etc., regardless of end-user technology limitations.	Any initiative system must be accessible to the broadest swath of the target jurisdiction possible; allow, invite, and proactively recruit legitimate users to the initiative; and be accessible from multiple platforms, operating systems, browsers, etc., regardless of end-user technology limitations. Few/some workstations dedicated only to initiative use are publicly available.	Any initiative system must be accessible to the broadest swath of the target jurisdiction possible; allow, invite, and proactively recruit legitimate users to the initiative; and be accessible from multiple platforms, operating systems, browsers, etc., regardless of end-user technology limitations. Many workstations dedicated only to initiative use are publicly available.
Security (SEC)			
SEC01: Risk Management	Risk assessments using the process outlined in NIST SP 800-37 (NIST Joint Task Force, 2018) and the controls specified in NIST SP 800-53 (NIST Joint Task Force, 2020) must be conducted and completed at least once before the adoption	Risk assessments using the process outlined in NIST SP 800-37 and the controls specified in NIST SP 800-53 must be conducted and completed at least twice—once before the implementation stage of the implementation-adoption	Risk assessments using the process outlined in NIST SP 800-37 and the controls specified in NIST SP 800-53 must be conducted and completed at least three times—once during the external conditions stage of the implementation-adoption

E-Democratic Government Success Requirements	**Baseline**	**Intermediate**	**Innovative**
	stage of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), and once annually thereafter.	model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), and once before the adoption stage of the same model—as well as twice annually thereafter. Risk management processes and/or controls supplemental to NIST SP 800-37 and NIST SP 800-53 are identified, analyzed, and discussed, but may not be formally incorporated into the risk management process.	model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), once before the implementation stage, and once before the adoption stage of the same model—as well as quarterly thereafter. Risk management processes and/or controls supplemental to NIST SP 800-37 and NIST SP 800-53 are formally incorporated into the risk management process.
SEC02: Cybersecurity Maturity	Cybersecurity maturity assessments must be conducted and completed against the NIST Cybersecurity Framework (Barrett, 2018) at least once before the adoption stage of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), and once annually thereafter.	Cybersecurity maturity assessments must be conducted and completed against the NIST Cybersecurity Framework (Barrett, 2018) at least twice—once before the implementation stage of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), and once before the adoption stage of the same model—as well as twice annually thereafter. Defense in Depth strategy is applied in some areas, and its application is well documented.	Cybersecurity maturity assessments must be conducted and completed against the NIST Cybersecurity Framework at least three times—once during the external conditions stage of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), once before the implementation stage, and once before the adoption stage of the same model—as well as quarterly thereafter. Defense in Depth strategy is applied wherever feasible, and its application is well documented, measured and evaluated.
SEC03: Disinformation Prevention	Initiative data is identified and labeled as accepted as truth, deemed false, or undetermined/questionable by no less than a simple majority of users. Identification/labeling of information is completed manually by users.	Initiative data is identified and labeled as accepted as truth, deemed false, or undetermined/questionable by no less than two-thirds of users. Identification/labeling of information is completed manually by users and could be assisted by machine learning automation.	Initiative data is identified and labeled as accepted as truth, deemed false, or undetermined/questionable by no less than three-quarters of users. Identification/labeling of information is completed automatically by machine learning automation and transparently reviewed thereafter by a democratically elected group of users.

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
Privacy (PRV) per Gerber et al. (2018)			
PRV01: Privacy attitude, concerns, and perceived risk	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding privacy attitudes, concerns, and perceived risk through tedious means, i.e., surveys, town hall meetings, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding privacy attitudes, concerns, and perceived risk using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding privacy attitudes, concerns, and perceived risk using technologies that have a nondigital equivalent, i.e., text mining social media posts and intra-initiative information. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.
PRV02: Privacy-related behavioral intention and willingness	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding privacy-related behavioral intention and willingness through tedious means, i.e., surveys, town hall meetings, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding privacy-related behavioral intention and willingness using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, evaluate, interpret, and address citizen sentiments regarding privacy-related behavioral intention and willingness using technologies that have a nondigital equivalent, i.e., text mining social media posts and intra-initiative information. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.
PRV03: Information disclosure behavior	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding information disclosure behavior through tedious means, i.e., surveys, town hall meetings, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding information disclosure behavior using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, evaluate, interpret, and address citizen sentiments regarding information disclosure behavior using technologies that have a nondigital equivalent, i.e., text mining social media posts and intra-initiative information. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.

E-Democratic Government Success Requirements	Baseline	Intermediate	Innovative
PRV04: Protection behavior and privacy settings	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding protection behavior and privacy settings through tedious means, i.e., surveys, town hall meetings, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, analyze, evaluate, interpret, and address citizen sentiments regarding protection behavior and privacy settings using entirely digital means, i.e., online survey, social media polling, data visualization, etc. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.	Collect, measure, evaluate, interpret, and address citizen sentiments regarding protection behavior and privacy settings using technologies that have a nondigital equivalent, i.e., text mining social media posts and intra-initiative information. Findings yielded from data collection and analysis spur changes, which are transparently implemented where sensible.

Table 4.3. Internally-related requirements and supporting literature for e-democratic government success requirements

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
E-Government Trends per Agawu (2017)		Agawu (2017)
Trust In Government (TGV) per Papp et al. (2020)		Aladwani & Dwivedi (2018) Avgerou (2013) Calderon et al. (2015) Gil-Garcia & Flores-Zúñiga (2020) Hossan & Ryan (2018) Jaidka & Ahmed (2015) Jamal et al. (2015) Papp et al. (2020) Petersen et al. (2020) Starke et al. (2020) Supriyanto et al. (2019) Tassabehji et al. (2007) Thomas (1998) Tolbert & Mossberger (2006)
TGV01: Behavioral trust	TGV02: Operational trust TGV03: Institutional trust All CEN01 requirements *except:* *CEN01.2: Minimal critical specification* CEN01.7: Multifunctionality CEN01.8: Support congruence CEN01.9: Transitional organization All CEN02 requirements *except:* *CEN02.1: Integration of tasks* *CEN02.2: Customization and personalization* *CEN02.4: Information retrieval and use* All SEC requirements All PRV requirements	Aladwani & Dwivedi (2018) Germonprez et al. (2017) Hanson et al. (2019) Kulkarni et al. (2006) Nemati et al. (2002) Papp et al. (2020) Tassabehji et al. (2007) Thomas (1998) Tolbert & Mossberger (2006)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
TGV01.1: Tasks	TGV02.1: Tasks TGV03.1: Tasks	Kulkarni et al. (2006) Nemati et al. (2002) Petersen et al. (2020)
TGV01.2: Knowledge	TGV02.2: Knowledge TGV03.2: Knowledge	Germonprez et al. (2017) Hanson et al. (2019) Petersen et al. (2020)
TGV01.3: Skills	TGV02.3: Skills TGV03.3: Skills	Germonprez et al. (2017) Hanson et al. (2019) Petersen et al. (2020)
TGV02: Operational trust	TGV01: Behavioral trust TGV03: Institutional trust All CEN requirements All SEC requirements All PRV requirements	Aladwani & Dwivedi (2018) Germonprez et al. (2017) Hanson et al. (2019) Papp et al. (2020) Petersen et al. (2020) Tassabehji et al. (2007) Thomas (1998) Tolbert & Mossberger (2006)
TGV02.1: Tasks	TGV01.1: Tasks TGV03.1: Tasks	Kulkarni et al. (2006) Nemati et al. (2002) Petersen et al. (2020)
TGV02.2: Knowledge	TGV01.2: Knowledge TGV03.2: Knowledge	Germonprez et al. (2017) Hanson et al. (2019) Petersen et al. (2020)
TGV02.3: Skills	TGV01.3: Skills TGV03.3: Skills	Germonprez et al. (2017) Hanson et al. (2019) Petersen et al. (2020)
TGV03: Institutional trust	TGV01: Behavioral trust TGV02: Operational trust All CEN requirements All SEC requirements All PRV requirements	Aladwani & Dwivedi (2018) Papp et al. (2020) Petersen et al. (2020) Tassabehji et al. (2007) Thomas (1998) Tolbert & Mossberger (2006)

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Supporting Literature**
TGV03.1: Tasks	TGV01.1: Tasks TGV02.1: Tasks	Kulkarni et al. (2006) Nemati et al. (2002) Petersen et al. (2020)
TGV03.2: Knowledge	TGV01.2: Knowledge TGV02.2: Knowledge	Germonprez et al. (2017) Hanson et al. (2019) Petersen et al. (2020)
TGV03.3: Skills	TGV01.3: Skills TGV02.3: Skills	Germonprez et al. (2017) Hanson et al. (2019) Petersen et al. (2020)
Citizen Engagement (CEN)		Bateman et al. (2011) Batlle-Montserrat et al. (2014) Bonacin et al. (2009) Cherns (1987) Hansson et al. (2014) Olphert & Damodaran (2007) Robertson (2005)
CEN01: Design using STT per Cherns (1987)		Ayyad (2017) Baxter & Somerville (2011) Cherns (1976) Cherns (1987) Clegg (2000) Hapsara (2016) Lyytinen & Newman (2008)

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Supporting Literature**
CEN01.1: Compatibility	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.8: Support congruence CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC03: Disinformation Prevention	Cherns (1987) Grönlund (2003) Mergel (2010) Nemati et al. (2002) Porwol et al. (2013)
CEN01.2: Minimal critical specification	TGV02: Operational trust TGV03: Institutional trust CEN01.9: Transitional organization CEN02.1: Integration of tasks CEN02.2: Customization and personalization CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing	Cherns (1987) Petersen et al. (2020) Porwol et al. (2013)
CEN01.3: Variance control	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.9: Transitional organization SEC02: Cybersecurity Maturity	Antoni et al. (2017) Barrett (2018) Cherns (1987) Hansson et al. (2014) NIST Joint Task Force (2020)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
CEN01.4: Boundary location	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.9: Transitional organization CEN02.1: Integration of tasks CEN02.2: Customization and personalization CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing CEN02.7: Diversity of users SEC01: Risk Management	Bateman et al. (2011) Cherns (1987) Davis (1989) Naicker & Mafaiti (2019)
CEN01.5: Information flow	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.6: Power and authority CEN02.2: Customization and personalization CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing SEC01: Risk Management SEC03: Disinformation Prevention	Antoni et al. (2017) Baxter & Sommerville (2011) Cherns (1987) NIST Joint Task Force (2020) Porwol et al. (2013)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
CEN01.6: Power and authority	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.5: Information flow CEN02.4: Information retrieval and use CEN02.6: Trust, control, and information sources CEN02.7: Diversity of users SEC01: Risk Management SEC03: Disinformation Prevention All PRV requirements	Antoni et al. (2017) Cherns (1987) Hansson et al. (2014) NIST Joint Task Force (2020)
CEN01.7: Multifunctionality	TGV02: Operational trust TGV03: Institutional trust CEN01.10: Incompletion	Cherns (1976) Cherns (1987) Davis (1989) Petersen et al. (2020) Porwol et al. (2013)
CEN01.8: Support congruence	TGV02: Operational trust TGV03: Institutional trust CEN01.1: Compatibility CEN02.3: Information gathering	Cherns (1976) Grönlund (2003)
CEN01.9: Transitional organization	TGV02: Operational trust TGV03: Institutional trust CEN01.2: Minimum critical specification CEN01.3: Variance control CEN01.4: Boundary location SEC01: Risk Management SEC02: Cybersecurity Maturity	Barrett (2018) Cherns (1987) NIST Joint Task Force (2020)
CEN01.10: Incompletion	CEN01.7: Multifunctionality TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust	Cherns (1976) Gil-Garcia & Flores-Zúñiga (2020)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
CEN02: Voter DSS Requirements per Robertson (2005)		Agawu (2017) Robertson (2005)
CEN02.1: Integration of tasks	TGV02: Operational trust TGV03: Institutional trust CEN01.2: Minimum critical specification CEN01.4: Boundary location CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing CEN02.6: Trust, control, and information sources CEN02.7: Diversity of users SEC03: Disinformation Prevention	Naicker & Mafaiti (2019) Porwol et al. (2013) Robertson (2005)
CEN02.2: Customization and personalization	TGV02: Operational trust TGV03: Institutional trust CEN01.2: Minimum critical specification CEN01.4: Boundary location CEN01.5: Information flow CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC03: Disinformation Prevention	Robertson (2005)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
CEN02.3: Information gathering	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.1: Compatibility CEN01.2: Minimum critical specification CEN01.4: Boundary location CEN01.5: Information flow CEN01.8: Support congruence CEN02.1: Integration of tasks CEN02.2: Customization and personalization CEN02.6: Trust, control, and information sources SEC03: Disinformation Prevention	Charalabidis et al. (2019) Nemati et al. (2002) Porwol et al. (2013) Robertson (2005)
CEN02.4: Information retrieval and use	TGV02: Operational trust TGV03: Institutional trust CEN01.1: Compatibility CEN01.2: Minimum critical specification CEN01.4: Boundary location CEN01.5: Information flow CEN01.6: Power and authority CEN02.1: Integration of tasks CEN02.2: Customization and personalization CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC03: Disinformation Prevention	Naicker & Mafaiti (2019) Porwol et al. (2013) Robertson (2005)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
CEN02.5: Information sharing	TGV02: Operational trust TGV03: Institutional trust CEN01.1: Compatibility CEN01.2: Minimum critical specification CEN01.4: Boundary location CEN01.5: Information flow CEN02.1: Integration of tasks CEN02.2: Customization and personalization CEN02.4: Information retrieval and use CEN02.6: Trust, control, and information sources SEC03: Disinformation Prevention All PRV requirements	Nemati et al. (2002) Porwol et al. (2013) Robertson (2005)
CEN02.6: Trust, control, and information sources	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.1: Compatibility CEN01.6: Power and authority CEN02.1: Integration of tasks CEN02.2: Customization and personalization CEN02.3: Information gathering CEN02.4: Information retrieval and use CEN02.5: Information sharing SEC03: Disinformation Prevention All PRV requirements	Charalabidis et al. (2019) Fu et al. (2018) Robertson (2005)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
CEN02.7: Diversity of users	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.2: Minimum critical specification CEN01.4: Boundary location CEN01.6: Power and authority CEN02.1: Integration of tasks SEC03: Disinformation Prevention	Hansson et al. (2014) Robertson (2005)
Security (SEC)		Barrett (2018) Gerber & von Somms (2008) McCumber (2004) NIST Joint Task Force (2018) NIST Joint Task Force (2020)
SEC01: Risk Management	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.4: Boundary location CEN01.5: Information flow CEN01.6: Power and authority CEN01.9: Transitional organization SEC02: Cybersecurity Maturity All PRV requirements	Gil-Garcia & Flores-Zúñiga (2020) Lidén (2013) McCumber (2004) NIST Joint Task Force (2018) NIST Joint Task Force (2020) Petersen et al. (2020)
SEC02: Cybersecurity Maturity	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.3: Variance control CEN01.9: Transitional organization SEC01: Risk Management All PRV requirements	Barrett (2018) Fraser & Vaishnavi (1997) Groat et al. (2012) Mell et al. (2016) Miron & Muita (2014) US Department of Homeland Security (2016)

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Supporting Literature**
SEC03: Disinformation Prevention	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.1: Compatibility CEN01.5: Information flow CEN01.6: Power and authority All CEN02 requirements	Farrell & Schneier (2018) Tesfay et al. (2018)
Privacy (PRV) per Gerber et al. (2018)		Gerber et al. (2018) NIST Joint Task Force (2020) Smith et al. (2011) Tesfay et al. (2018)
PRV01: Privacy attitude, concerns, and perceived risk	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.6: Power and authority CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC01: Risk Management SEC02: Cybersecurity Maturity	Gerber et al. (2018) Smith et al. (2011)
PRV02: Privacy-related behavioral intention and willingness	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.6: Power and authority CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC01: Risk Management SEC02: Cybersecurity Maturity	Gerber et al. (2018) Smith et al. (2011)

E-Democratic Government Success Requirements	Internally Related Requirements	Supporting Literature
PRV03: Information disclosure behavior	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.6: Power and authority CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC01: Risk Management SEC02: Cybersecurity Maturity	Gerber et al. (2018) Smith et al. (2011)
PRV04: Protection behavior and privacy settings	TGV01: Behavioral trust TGV02: Operational trust TGV03: Institutional trust CEN01.6: Power and authority CEN02.5: Information sharing CEN02.6: Trust, control, and information sources SEC01: Risk Management SEC02: Cybersecurity Maturity	Gerber et al. (2018) Smith et al. (2011)

CHAPTER 5

EVALUATION

This chapter contains detailed evaluations of the E-Democratic Government Success Framework artifact and discussion about those evaluations. It is organized into four tables. Table 5.1 shows the artifact's requirements benchmarked to past and current US E-Democracy initiatives discussed in the literature review—namely, (a) the Obama Administration's *We The People* monitorial platform launched in 2011, (b) the US Patent and Trademark Office's crowdsourced art review in 2012, (c) the White House Office of Science and Technology's crowdsourced strategic innovation policy report in 2014, (d) the *Boston311* platform since 2009, and (e) the lawsourced bill by California State Congressman Mike Gatto in 2013. Table 5.2 shows relevant cybersecurity frameworks and theories used in this work contextually mapped to the artifact's requirements. Table 5.3 applies the artifact's requirements to a synthetic lawsourcing platform for scenario creation evaluation. Finally, Table 5.4 applies defense in depth theory to the artifact through informed argument by identifying which of the artifact's requirements are related to others and justifying their relationship.

Table 5.1. Benchmarking through gap analysis between artifact and past e-democracy initiatives

E-Democratic Government Success Requirements	Noncompliant	Baseline	Intermediate	Innovative
E-Government Trends per Agawu (2017)	(b) No trends were present. (c) No trends were present.	(a) Digitized service loop, reporting system from citizens to government. (d) Digitizes service loop, reporting system between citizens and government.	(e) Digitized service loop with citizens crafting law proposals alongside legislators and could have created a nondigital equivalent if the initiative continued.	
Trust In Government (TGV) per Papp et al. (2020)	(a-e) Citizen trust in government sentiment measuring was not conducted according to public knowledge.			

E-Democratic Government Success Requirements	**Noncompliant**	**Baseline**	**Intermediate**	**Innovative**
TGV01: Behavioral trust	(a-e) See TGV.			
TGV01.1: Tasks	(a-e) See TGV.			
TGV01.2: Knowledge	(a-e) See TGV.			
TGV01.3: Skills	(a-e) See TGV.			
TGV02: Operational trust	(a-e) See TGV.			
TGV02.1: Tasks	(a-e) See TGV.			
TGV02.2: Knowledge	(a-e) See TGV.			
TGV02.3: Skills	(a-e) See TGV.			
TGV03: Institutional trust	(a-e) See TGV.			
TGV03.1: Tasks	(a-e) See TGV.			
TGV03.2: Knowledge	(a-e) See TGV.			
TGV03.3: Skills	(a-e) See TGV.			
Citizen Engagement (CEN)				
CEN01: Design using STT per Cherns (1987)	(a-e) See CEN01 subcategories.			
CEN01.1: Compatibility	(b-c) No policymaking stages were digitized.	(a) Agenda setting was partially digitized (agenda proposals were digitized, decision making in agenda setting was limited to 100,000 signatures on a petition). (d) Agenda setting is digitized through bidirectional communication between citizens and government. (e) Analysis and creating the policy were digitized, but the policy was never implemented, and it is unclear how the agenda was set.		

E-Democratic Government Success Requirements	Noncompliant	Baseline	Intermediate	Innovative
CEN01.2: Minimal critical specification	(a-e) Citizen sentiments were not meaningfully collected and addressed. (a) required 100,000 signatures for response and that did not guarantee action, (d) does not conduct sentiment analysis according to public knowledge, and (e) attempted and failed in remedying an issue with policy.			
CEN01.3: Variance control	(a-e) In each initiative, there was always a power dynamic at play. In (a), 100,000 signatures were required for response which did not guarantee action. In (b-c), the initiative managers selected and compiled the result. In (d), it is unclear how reported issues are prioritized. And in (e), whoever set the agenda had more power than other participants.			
CEN01.4: Boundary location	(a-e) None of the initiatives provided a means to easily share information, other than conventional internet techniques (i.e., sharing a URL).			
CEN01.5: Information flow	(a-c, e) No information was provided during system design and engineering or organizational change activities. (d) The Boston Mayor's office engaged in community meetings and town halls during design, but the extent to which relevant information was provided is unclear. Further, no mapping of			

E-Democratic Government Success Requirements	**Noncompliant**	**Baseline**	**Intermediate**	**Innovative**
	information flow was publicly disclosed.			
CEN01.6: Power and authority	(a-e) None of the initiatives met the spirit of the requirement, as each initiative had one or more power users that were not explicitly elected for that role.			
CEN01.7: Multifunctionality	(a-e) Each initiative's managers could have theoretically added or modified new roles, but there is no public record of any gap analysis between existing roles and organizational, governmental, and constituent needs.			
CEN01.8: Support congruence	(a-e) None of the initiatives show any public knowledge of support role gap analysis.			
CEN01.9: Transitional organization	(a-e) Whether initiative managers planned and designed changes before they occurred is unknown, but no gap analysis results were publicly shared.			
CEN01.10: Incompletion	(a-e) According to public knowledge, it does not appear as if any of the initiatives were evaluated for improvement.			
CEN02: Voter DSS Requirements per Robertson (2005)	(a-e) See CEN02 subcategories.			
CEN02.1: Integration of tasks	(a-e) None of the initiatives conducted vast processing or monitoring of social media data, but some provided feedback in varying situations per public knowledge.			

E-Democratic Government Success Requirements	Noncompliant	Baseline	Intermediate	Innovative
CEN02.2: Customization and personalization	(a-e) Although the extent of customization and personalization is unknown for each initiative from public knowledge, much more in this requirement could have been done in each initiative. For example, (a) was merely a web form and (e) used a third-party website that was not designed specifically for its purpose.			
CEN02.3: Information gathering	(a-e) According to public knowledge, none of the initiatives meaningfully organized or simplified information gathering.			
CEN02.4: Information retrieval and use	(a-e) According to public knowledge, none of the initiatives meaningfully organized or simplified information retrieval and use, aside from conventional computer techniques (i.e., using third-party search engines).			
CEN02.5: Information sharing	(a-d) None of these initiatives allow for the identification of and communication with other users.	(e) Although likely unintentional, the third-party website this initiative was hosted on, *Wikispaces*, allowed for user identification and communication. However, no knowledge management was conducted per public knowledge.		
CEN02.6: Trust, control, and information sources	(a-e) None of the initiatives meaningfully allowed users to define their identities, participation and browsing preferences, etc.			

E-Democratic Government Success Requirements	**Noncompliant**	**Baseline**	**Intermediate**	**Innovative**
CEN02.7: Diversity of users		(a-e) Each of the initiatives did not explicitly exclude members of their respective jurisdictions from participating, but none of the initiatives offered public workstations per public knowledge.		
Security (SEC)				
SEC01: Risk Management	(a-e) None of the initiatives publicly communicated that risk assessments were conducted or provided any results. Further, it does not appear any tracking to digital government models was completed by any initiatives.			
SEC02: Cybersecurity Maturity	(a-e) None of the initiatives publicly communicated that cybersecurity maturity assessments were conducted or provided any results. Further, it does not appear any tracking to digital government models was completed by any initiatives.			
SEC03: Disinformation Prevention	(a-e) None of the initiatives publicly identified information as true, false, or inconclusive.			
Privacy (PRV) per Gerber et al. (2018)	(a-e) Citizen privacy sentiment measuring was not conducted according to public knowledge.			
PRV01: Privacy attitude, concerns, and perceived risk	(a-e) See PRV.			
PRV02: Privacy-related behavioral	(a-e) See PRV.			

E-Democratic Government Success Requirements	Noncompliant	Baseline	Intermediate	Innovative
intention and willingness				
PRV03: Information disclosure behavior	(a-e) See PRV.			
PRV04: Protection behavior and privacy settings	(a-e) See PRV.			

Predictably, past and current US E-Democracy initiatives do not fare well against the artifact framework. Case studies (b) and (c) immediately fail to meet the requirements of the framework's scope, in that they did not increase access to content, digitize the service loop, or create/expand government function to include a nondigital equivalent. However, for evaluation purposes, these case studies were assessed throughout the entire framework, nonetheless. Even case studies (a) and (d), thought to be the most 'conventional' E-Democracy initiatives, are noncompliant with four out of the five larger categories—mostly due to the lack of transparency and neglecting to include citizens within the design process. Remarkably, the same noncompliance in four out of five categories is true of the most 'innovative' US E-Democracy initiative: case study (e). Although this case study arguably straddles the baseline and intermediate standards in the E-Government G2C Trends category, noncompliance in the four remaining categories is caused by the same issues: either there was no public information to prove compliance, or the initiative system never grew to include many required features as citizens were never involved in the design process. At the same time, none of these initiatives meaningfully increased civic engagement, so ideally, they all should arguably fail an audit against this framework.

Table 5.2 maps the cybersecurity frameworks and theories discussed in the artifact to the artifact's requirements to clearly demonstrate the context with which each framework and theory is used. Further, this mapping allows users to see which requirements and controls are not a part of current cybersecurity frameworks and theories, inherently justifying the need for this framework.

Table 5.2. Benchmarking through contextual mapping of relevant cybersecurity frameworks and theories

Cybersecurity Framework/Theory	E-Democratic Government Success Requirement and Description
McCumber Cube Model (McCumber, 2004)	SEC01: Assists the risk management process to envision unforeseen risks.
Defense in Depth (US National Security Agency, 2015)	SEC02: A less comprehensive measurement tool for cybersecurity maturity, but more so a strategy recommended by the NSA for increasing cyber resilience.
NIST Cybersecurity Framework (Barrett, 2018)	CEN01.3: Controls variances through enforced persistent anomaly detection.
	CEN01.9: Transitional organization is managed through enforced information protection procedures.
	SEC02: Principal evaluation tool to measure cybersecurity maturity.
NIST SP 800-37 (NIST Joint Task Force, 2018)	SEC01: Denotes the risk management process and lifecycle; used in tandem with NIST SP 800-53.
NIST SP 800-53 (NIST Joint Task Force, 2020)	CEN01.3: Controls variances through principles like separation of duties, principle of least privilege, etc.
	CEN01.5: Information flow is enforced through approved authorizations through organizational policy.
	CEN01.6: Power and authority are enforced through policies supporting least privilege and non-repudiation.
	CEN01.9: Transitional organization is enforced through policies supporting configuration and change management.
	SEC01: Identifies hundreds of controls for security and privacy of federal information systems and used in tandem with NIST SP 800-37.
NIST SP 800-181, NICE Framework (Petersen et al., 2020)	TGV: Assists the framework design in helping envision workforce roles based around increasing trust in government.
	SEC01: Assists the risk management process to envision tasks, skills, and knowledge required for a cybersecurity workforce in identifying and closing bureaucratic gaps.

Although more connections are inevitable with time, there are some computer security themes that users of any platform can take away from this analysis. First, models and theories like the McCumber Cube and defense in depth can be used to envision unforeseen risks and harden organizations and their systems against those risks (McCumber, 2004; US National Security Agency, 2015). Second, the NIST Cybersecurity Framework is better suited for evaluating cybersecurity maturity—and not for helping organizations become more secure in cyberspace (Barrett, 2018; Miron & Muita, 2014). Third, the risk management process and controls in NIST SP 800-37 and 800-53 are what conventional computer security practices look like, and these documents are periodically updated and revised to help users foresee and mitigate new risks (NIST Joint Task Force, 2018; NIST Joint Task Force, 2020). Finally, the NICE Framework is most useful in defining workforce roles for cybersecurity in new or emerging areas.

Table 5.3 applies the framework artifact's requirements to a synthetic lawsourcing initiative as scenario creation, which further demonstrates use of and compliance to the framework. The lawsourcing evaluation has some minor and major requirements greyed out, as there is insufficient literature to inform guidance in these areas. These omitted requirements include the NICE Framework application (tasks, knowledge, skills) for TGV, the major categories of CEN, CEN01, CEN02, and SEC, and the minor PRV requirements. In the case of the NICE Framework application, there is no other record of democracies using such advanced sentiment analysis. For this reason, it seems appropriate to omit guidance until a pilot study in a production environment can occur and be analyzed to inform such guidance. In the case of CEN, CEN01, CEN02, and SEC, all the offered guidance pertains to minor requirements as these major requirements only require meeting the baseline standard of each's minor requirements. Finally, the minor PRV requirements suffer from the same issue as TGV; due to the lack of literature regarding user privacy expectations on public sector technological platforms, it seems appropriate to omit specific guidance on each privacy area until a pilot study in a production environment can occur and be analyzed to inform such guidance.

Table 5.3. Scenario creation through lawsourcing

E-Democratic Government Success Requirements	**Application to Synthetic Lawsouring Initiative**
E-Government Trends per Agawu (2017)	The initiative can increase access to relevant information and content by publishing and updating jurisdiction-specific existing and proposed laws onto its platform for review by citizens. Rather than interfacing directly or by other means with lawmakers, the initiative can digitize the service loop by giving citizens the ability to submit feedback through the platform, specific to individual laws, proposals, sections, lines, etc. Finally, the initiative can create a government function without a nondigital equivalent through the ability to craft and edit existing laws or new proposals with others by using the platform.
Trust In Government (TGV) per Papp et al. (2020)	Government officials responsible for the initiative may have to manually administer the collection, measurement, analysis, evaluation, and interpretation of citizen trust in government sentiments initially if no other means are available. Eventually, the lawsourcing platform can incorporate or otherwise digitize/automate the collection and measurement of data, and the evaluation, interpretation, and eventual predictive functionality stemming from that data can occur either within or outside the lawsourcing platform—so long as the data informing that evaluation, interpretation, and prediction comes from the lawsourcing platform and other legitimate data sources. Government officials should be reasonably responsive to interpretations and conclusions taken from the data analyses and should adapt government and governance to align with those conclusions when possible.
TGV01: Behavioral trust	Government officials should continually seek to improve their behavioral trust with citizens by using the knowledge acquired through data analysis of citizen sentiments to make prediction through decision support and knowledge management possible.
TGV01.1: Tasks	
TGV01.2: Knowledge	
TGV01.3: Skills	
TGV02: Operational trust	Government officials and agencies responsible for processes should continually seek to improve their operational trust with citizens by using the knowledge acquired through data analysis of citizen sentiments to make prediction through decision support and knowledge management possible.
TGV02.1: Tasks	
TGV02.2: Knowledge	
TGV02.3: Skills	
TGV03: Institutional trust	Governmental institutions and/or their agents should continually seek to improve the capability of increasing behavioral trust by using the knowledge acquired to make prediction through decision support and knowledge management possible.
TGV03.1: Tasks	
TGV03.2: Knowledge	
TGV03.3: Skills	
Citizen Engagement (CEN)	
CEN01: Design using STT per Cherns (1987)	

E-Democratic Government Success Requirements	Application to Synthetic Lawsouring Initiative
CEN01.1: Compatibility	The objectives of the lawsourcing initiative may initially be to digitize only a few of the policymaking stages. However, the goal must be to digitize all policymaking stages over time. Being a lawsourcing platform, the policymaking stages are the most critical to compatibility and stakeholders should prioritize them accordingly. There are clearly risks to success with a platform that claims it does lawsourcing yet does not function that way.
CEN01.2: Minimal critical specification	In applying the NICE Framework (Petersen et al., 2020) to lawsourcing, the tasks, jobs, and roles of the initiative should only derive from what is required to facilitate lawsourcing activities (namely those identified by Porwol et al., 2013)—nothing less and nothing more. Likely this would require database design and management, website design and management, and citizen trust-in-government sentiment analysis at a minimum. However, the tasks, jobs, and roles of the initiative should expand over time.
CEN01.3: Variance control	No single, un-elected user of an E-Democratic Government platform should have a higher or lower status when decisions are taken. If un-elected power users can override or in any way alter the decisions made by typical users, the platform facilitates oligarchy, not democracy. Initiative manager could address this perception by providing transparency into how variances are controlled, demonstrating that each user participant in the initiative is equal, and that each power user is unable to participate according to the separation of duties principle.
CEN01.4: Boundary location	The lawsourcing initiative must not omit information, knowledge, learning mediums, or sources unless the target community democratically decides to disqualify. Otherwise, the lawsourcing initiative should allow incorporation of information, knowledge, learning mediums, and sources so that such incorporation is easy and straightforward. Modeling and evaluating where initiative information comes from and how that incorporation of external information can be improved should occur as often as possible, increasing in rate over time.
CEN01.5: Information flow	Transparency is key to the success of any E-Democratic Government initiative due to its dependency on trust, and in turn, trust's dependency on success. This remains true through the demand phase of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020); users may see a lack of transparency as a sign of nefarious intentions, which itself could drive away users. Information in an E-Democratic Government platform should flow from citizens to government, and from government to citizens, in a simultaneous and healthy fashion whereby the remainder of the requirements in this framework are sufficiently met. In a lawsourcing platform, citizens should contribute towards the policy-making stages, and government should be responding to contributions and other expressed sentiments, processing those contributions, reporting aggregated information (like the highest-contributing individuals) back to the users, and providing the ability for users to view sources of information.
CEN01.6: Power and authority	In any technological system, there must be one or more individuals that have administrative access to applications, databases, other software, and hardware that supports the initiative. These power users must be democratically elected to short terms and must not use the platform as required by separation of duties principle. Further, policies regarding power users and procedures describing how those policies are implemented should be transparent to the users of the platform. Transparency is key to the success of any initiative due to its dependency on trust, and in turn, trust's dependency on success. This remains true through the demand phase of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020); users may see a lack of transparency as a sign of nefarious intentions, which itself could drive away users.

E-Democratic Government Success Requirements	**Application to Synthetic Lawsouring Initiative**
CEN01.7: Multifunctionality	The agility of any E-Democratic Government initiative and its systems is crucial to its continuity, and the agility of a lawsourcing initiative and its systems not only informs the extent of its success, but also informs the agility of its jurisdiction's policy creation. If external conditions, or any other components of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), are changed in some way, the need for new or modified roles may be critical to the continued success of the initiative. Further, users should be consulted in decisions regarding initiative role creation or modification.
CEN01.8: Support congruence	The lawsourcing initiative's support systems' compatibility with policy-making is crucial to the initiative's continuity. For example, imagine users needing help with the initiative's mobile application, but the initiative does not provide support for the mobile application as it is run through a third party, and the third party does not offer support. In this case, the user may decide to leave the platform entirely if they are unwilling or unable to further use the application—even if the application was available through another means, such as a website through a browser. If external conditions, or any other components of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), are changed in some way, the need for retiring, creating, and/or modifying support systems may be critical to the continued success of the initiative.
CEN01.9: Transitional organization	Like how agility of an organization is crucial to its continuity, the agility of a lawsourcing initiative would not only inform its own success but also the agility of its jurisdiction's policy creation. If external conditions, or any of the other phases of the implementation-adoption model of Digital Government Success from Gil-Garcia & Flores-Zúñiga (2020), are changed in some way, the need for change may be detrimental to the continued success of the initiative.
CEN01.10: Incompletion	The lawsourcing initiative, like any other E-Democratic Government initiative, should consistently and continually evaluate itself against this framework. Adhering to this framework may not always be possible or feasible, and the evaluation process may not always be straightforward. However, it is tantamount to the continued success and improvement of E-Democratic Government initiatives that managers understand the gaps between the status quo and best practices and publicly communicate those deficiencies, at a minimum.
CEN02: Voter DSS Requirements per Robertson (2005)	
CEN02.1: Integration of tasks	Porwol et al. (2013) identify tools in social software infrastructure that enable policy making and agenda creation; multi-source knowledge extraction and management; discussion control, exploration, and analytics; and mission control. Lawsourcing as an activity is easily comparable to these tools, and each of these should integrate into one platform. Of course, it is not best practice to run multiple services on the same hardware; where there are multiple systems (e.g., one for policy debate and contributions, one for monitoring and processing social media and participation data), these systems should be accessible from a single homepage. For example, E-Democracia is a homepage for Brazil's E-Democracy platform that links to four separate systems (translated from Portuguese): *Interactive Audiences*, *WikiLegis*, *e-monitor*, and *Participatory Agenda*.

E-Democratic Government Success Requirements	Application to Synthetic Lawsouring Initiative
CEN02.2: Customization and personalization	Lawsourcing expects users to evaluate existing legislation, craft proposed edits or new legislation, and evaluate other proposed edits and new legislation. Accordingly, the ability for the user to configure their own filters, searches, preferences, and profiles in tailoring their own experience within the lawsourcing platform is critical to its success. Over time, users should be able to tailor their experience in a more complex way, such as by using developer application programming interfaces (API) of the initiative software to further program beyond what the website's graphical user interface will allow.
CEN02.3: Information gathering	Users' ability to gather, identify, organize, and filter information directly and indirectly from any source is crucial to the success of any E-Democratic Government initiative, but especially to lawsourcing due to its close connection to policy-making. Like academic plagiarism software, the initiative system should be able to identify and label unlabeled information that exists elsewhere on the internet. This identification allows initiative managers to conduct data analysis and use knowledge management systems much more efficiently. Separately, lawsourcing expects users to evaluate current and proposed legislation but does not inherently account for users with the inability to interpret lengthy legal texts. Accordingly, legal text mining should be incorporated into the system over time, as this functionality can automatically summarize any legal texts to help with interpretation.
CEN02.4: Information retrieval and use	Users' ability to use tools within and outside of the initiative system to categorize, annotate, and associate gathered information to issues, groups, and/or individuals is crucial to the success of any E-Democratic Government initiative, but especially to lawsourcing due to its close connection to policy-making. After analyzing information, lawsourcing expects users to craft new legal proposals or recommend modifications to existing legislation and proposals, so sources of gathered information must be identified to prevent disinformation and assist in knowledge management. Identification of sources for information must occur once the information is introduced to the initiative system, and for the duration that information remains on the initiative system.
CEN02.5: Information sharing	Users' abilities to identify people and groups that can assist in decision support; participate with those people and groups via discussion; share and flag information and filters easily; and use external tools for initiative information are crucial to the success of any E-Democratic Government initiative, but especially to lawsourcing due to its close connection to policy-making. After analyzing information, lawsourcing expects users to craft new legal proposals or recommend modifications to existing legislation and proposals, so information sharing (empowered by knowledge management) is key to the accuracy of the lawsourcing process.
CEN02.6: Trust, control, and information sources	Users' ability to define and protect their identities, participation patterns, and information as private is crucial to the success of any E-Democratic Government initiative, but especially to lawsourcing due to its close connection to policy-making. Lawsourcing expects users to craft new legal proposals or recommend modifications to existing legislation and proposals, so it is crucial to user privacy, trust in government, and initiative success that identities, patterns, and information that users define as private be available only according to that user's preferences.
CEN02.7: Diversity of users	The broadest possible swath of the population must be invited to accessibly use the initiative system through policy, process, and technology, as this is critical to the success of any E-Democratic Government initiative. As a democratic lawsourcing platform expects citizens to craft and edit policy together, no single user or subset of users ought to be excluded from participating—unless democratically agreed upon (e.g., nonvoters or noncitizens). Inevitably, populations will include those who are resilient, uncomfortable, and/or otherwise incapable of participating using technology. Government-provided public-use technology stations with resource staff available for assistance are recommended to bridge this divide.

E-Democratic Government Success Requirements	**Application to Synthetic Lawsouring Initiative**
Security (SEC)	
SEC01: Risk Management	The risk management process in NIST SP 800-37 (NIST Joint Task Force, 2018) and the controls in NIST SP 800-53 (NIST Joint Task Force, 2020) may be too costly for a smaller jurisdiction to conduct entirely, either in human or fiscal resources. However, as noted in Part One's Target Audience subsection of this framework, when meeting the baseline standards of requirements (other than Agawu's (2017) E-Government G2C Trends) is unattainable due to lack of resources, stakeholders should identify which requirements are unattainable, determine a feasible alternative baseline standard that is relevant to the success requirement, and justify its substitution to the target jurisdiction's community. In the case of risk management for a lawsourcing platform under minimal resources, the initiative's administration should still incorporate the NIST SP 800-37 risk management process, but with tighter scrutiny in the third step (select) in that only highest-level priority controls should be selected. This prioritization is partially completed, except for controls added in the fifth revision, if the user references NIST SP 800-53, revision four. Here, controls were prioritized as P1, P2, P3, or P0. Administration should ensure that, at minimum, P1 controls are selected in the NIST SP 800-37 risk management processes' third step. Unfortunately, the authors did not complete this prioritization in the fifth revision, so mapping of the added NIST SP 800-53, revision five controls to priority levels should be completed. Over time, the number of controls to select should increase, eventually incorporating P2, P3, and P0 controls, and/or the entirety of NIST SP 800-53, revision five controls. As this substitution cannot occur in the intermediate or innovative levels, users should then seek to expand the controls selected to address newly discovered risks specific to E-Democratic Government that the NIST 800-53 controls do not address.
SEC02: Cybersecurity Maturity	Cybersecurity maturity may be underdeveloped when an initiative is in its early stages or due to numerous factors. However, baseline compliance only requires conducting a maturity assessment on a continuous basis to allow for tracking and planning to improve cybersecurity maturity. This adherence to the baseline standard of this requirement is critical to the success and legitimacy of any E-Democratic Government initiative. In SEC01, it is recommended that users determine an alternative baseline standard in the event compliance is unattainable due to lack of resources and communicate/justify the substitution with the target jurisdiction's community. However, similar substitution is not explicitly permitted for this requirement. This is because nearly all the NIST Cybersecurity Framework (Barrett, 2018) subcategories are mapped to related NIST SP 800-53, revision four, controls, and most of those controls are already assigned priority P1. In other words, because a relevant substitution has already occurred with the SEC01 baseline standard, another substitution in the same category should be avoided.
SEC03: Disinformation Prevention	In the lawsourcing initiative, or any other E-Democratic Government, the process of disinformation prevention through the identification and labeling of initiative information is straightforward, albeit the effects of disinformation prevention and the actual identification and labeling of information is challenging. It is highly recommended that citizens democratically decide on an information labeling schema and collectively determine outcomes of each determination. In less comprehensive initiatives that incorporate access to content or digitization of the service loop only, disinformation prevention may become even more challenging as there may not be an obvious way to identify initiative information. When only access to content is provided, a democratically elected board should oversee the validity of information provided on the platform, and users should be able to publicly comment, rate, and discuss validity of information and users through reputational systems. When an initiative only incorporates digitization of the service loop, transparency should be the primary focus of disinformation prevention.

E-Democratic Government Success Requirements	**Application to Synthetic Lawsouring Initiative**
Privacy (PRV) per Gerber et al. (2018)	In lawsourcing, users can contribute their ideas about existing and new policies. Information disclosure could include users' political, economic, social, and other opinions or attributes that may expose users' identities. Users may be hesitant to meaningfully interact with initiative systems based on their own past experiences with other technologies, the attitudes formed from those experiences, and their direct and indirect experience with initiative systems. There may be a persistent percentage of the target jurisdiction's population of eligible, legitimate users that refuse to participate regardless of any actions, changes, or policies. Even still, understanding and addressing user privacy-related behavioral intentions and willingness is critical to the success of the initiative—especially in cases where participation is low.
PRV01: Privacy attitude, concerns, and perceived risk	
PRV02: Privacy-related behavioral intention and willingness	
PRV03: Information disclosure behavior	
PRV04: Protection behavior and privacy settings	

Table 5.4 demonstrates the application of defense in depth to the artifact by identifying which of the framework's requirements are related to each other—thereby reinforcing one another—and justifying each connection with informed argument and/or logical reasoning. Again, some of the major and minor categories are greyed out as there is insufficient literature to inform guidance in these areas, or there are logical overlaps. For example, the E-Government Trends per Agawu (2017) requirement arguably relates to each of the requirements in this framework, but it feels redundant to explain a point touched on repeatedly in this work. TGV, CEN01, CEN02, and SEC felt appropriate to compare individually, while the lack of literature in privacy made it much easier to discuss PRV requirements altogether. Often, relationships are demonstrated through a negative argument, i.e., 'if *x* requirement was not met, then *y* requirement would suffer, decrease, become impossible, etc.' Again, this strategy was used to more easily demonstrate the connections found in this research, and the connections identified are by no means exhaustive.

Table 5.4. Application of defense in depth theory through mapping redundancy of internal requirements

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
E-Government Trends per Agawu (2017)		
Trust In Government (TGV) per Papp et al. (2020)		
TGV01: Behavioral trust	TGV02: Operational trust	All modes of trust relate to each other as literature identifies trust in government as a holistic concept (i.e., a citizen expressing distrust in a government agent who oversees an institution is less likely to trust that institution) and that this trust-building occurs over time (Thomas, 1998; Tassabehji et al., 2007).
	TGV03: Institutional trust	*See TGV01–TGV03.*
	CEN01.1: Compatibility	If an initiative is branded as E-Democratic Government but does not digitize one or more policy-making stages, this is likely to affect all dimensions of trust in government for the responsible government personnel, processes, and institutions negatively. Citizens will expect to use an E-Democratic Government platform primarily for digital policymaking or its support systems, and if they are unable to do so, they will distrust the people, processes, and institutions that deceived them.
	CEN01.3: Variance control	If unelected participants do not all have the same status when decisions are taken, or if social/bureaucratic boundaries are reflected in user accounts, citizens will distrust the people, processes, and institutions that facilitated an unjust system of digital policy-making.
	CEN01.4: Boundary location	If initiative system boundaries are drawn in a way to hinder learning and information or knowledge sharing, citizens will distrust the people, processes and institutions that helped facilitate those boundaries.
	CEN01.5: Information flow	If initiative information is not provided to participants during critical activities or when they otherwise require it, and if these information flows are not transparently modeled, citizens will distrust the people, processes, and institutions that obscured the system.
	CEN01.6: Power and authority	If some unelected participants—or elected power users that overstay their welcome—have more power than other than other unelected participants, citizens will distrust the people, processes, and institutions that facilitated an unjust system of digital policy-making. The same distrust will occur if elected power users do not have access to required resources; as elected officials, they will likely communicate the restricted access to all participants, thereby eroding trust.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	CEN01.10: Incompletion	If the initiative system is not reevaluated to consider changes to external conditions or other findings from audits against this framework, citizen will distrust the people, processes, and institutions that fail to adapt the initiative system to their needs.
	CEN02.3: Information gathering	If participants are unable to freely gather, identify, organize, and filter information, their role in digital policy-making becomes unnecessarily difficult. This undue difficulty will cause citizens to distrust the people, processes, and institutions that did not facilitate ease of use of the initiative system.
	CEN02.5: Information sharing	If the initiative system does not support communal attitude, opinion, and choice formation through information sharing abilities, the citizens will distrust the people, processes, and institutions that did not facilitate ease of use of the initiative system.
	CEN02.6: Trust, control, and information sources	If participants are unable to define aspects of their participation as private, citizens will distrust the people, processes, and institutions that systematically publicized their participation. The same distrust will occur if participants cannot select and categorize their preferred information sources; citizens will distrust the people, processes, and institutions that appear to prefer certain information sources over those preferred by participants.
	CEN02.7: Diversity of users	If the initiative system is not accessible to one or more subsets of the jurisdiction's population—whether by design, secrecy, platform incompatibility, or otherwise—citizens will distrust the people, processes, and institutions that selectively include participants under the guise of democracy.
	All SEC requirements	Risk management, cybersecurity maturity, and disinformation prevention are necessary for maintaining and increasing trust in government. If the initiative system was compromised and data was changed or stolen due to poor risk management or insufficient cybersecurity maturity, citizens would distrust the people, processes, and institutions which did not defend their data. The same distrust will occur if the initiative system has no means to remove disinformation; citizens will no longer trust and use the system if it is perceived to be overcome with falsehoods.
	All PRV requirements	Collection, measurement, analysis, evaluation, and interpretation of citizen sentiments are required in both trust in government and privacy sections of this framework. Privacy and trust in government are inherently connected, as a system which does not keep citizen's data private when they define it as such will see citizens distrust the people, processes, and institutions that did not safeguard their preferences.
TGV01.1: Tasks	TGV02.1: Tasks	Required tasks are the same (collection, measurement, analysis, evaluation, interpretation, and eventually prediction of citizen trust sentiments) but the targets are different.
	TGV03.1: Tasks	*See TGV01.1–TGV02.1.*
TGV01.2: Knowledge	TGV02.2: Knowledge	Required knowledge is the same (external conditions and maintaining/increasing trust in government) but the targets are different.
	TGV03.2: Knowledge	*See TGV 01.2–TGV02.2.*

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
TGV01.3: Skills	TGV02.3: Skills	Required skills are the same (data collection and analysis, ability to navigate, understand, and adapt government) but the targets are different.
	TGV03.3: Skills	*See TGV01.3–TGV2.3.*
TGV02: Operational trust	TGV01: Behavioral trust	*See TGV01–TGV03.*
	TGV03: Institutional trust	*See TGV01–TGV03.*
	All CEN requirements	If citizens' involvement and participation are not a central force in design of or evaluation of the initiative, citizens will distrust the processes and institutions that excluded them. Only so many parts of a system can logically be attributed to government agents, and although agents obviously bear responsibility in overseeing initiatives' processes and institutions, this framework does not connect some CEN requirements with TGV01: Behavioral Trust. This is because operational and institutional trust are more directly relevant for these requirements.
	All SEC requirements	*See TGV01—All SEC requirements.*
	All PRV requirements	*See TGV01—All PRV requirements.*
TGV02.1: Tasks	TGV01.1: Tasks	*See TGV01.1–TGV02.1.*
	TGV03.1: Tasks	*See TGV01.1–TGV02.1.*
TGV02.2: Knowledge	TGV01.2: Knowledge	*See TGV 01.2–TGV02.2.*
	TGV03.2: Knowledge	*See TGV 01.2–TGV02.2.*
TGV02.3: Skills	TGV01.3: Skills	*See TGV01.3–TGV2.3.*
	TGV03.3: Skills	*See TGV01.3–TGV2.3.*
TGV03: Institutional trust	TGV01: Behavioral trust	*See TGV01–TGV03.*
	TGV02: Operational trust	*See TGV01–TGV03.*
	All CEN requirements	*See TGV02—All CEN requirements.*
	All SEC requirements	*See TGV01—All SEC requirements.*
	All PRV requirements	*See TGV01—All PRV requirements.*
TGV03.1: Tasks	TGV01.1: Tasks	*See TGV01.1–TGV02.1.*
	TGV02.1: Tasks	*See TGV01.1–TGV02.1.*
TGV03.2: Knowledge	TGV01.2: Knowledge	*See TGV01.2–TGV02.2.*
	TGV02.2: Knowledge	*See TGV01.2–TGV02.2.*
TGV03.3: Skills	TGV01.3: Skills	*See TGV01.3–TGV02.3.*
	TGV02.3: Skills	*See TGV01.3–TGV02.3.*
Citizen Engagement (CEN)		

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
CEN01: Design using STT per Cherns (1987)		
CEN01.1: Compatibility	All TGV requirements	*See TGV01—CEN01.1.*
	CEN01.8: Support congruence	E-Democratic Government seeks to increase civic participation through technology, and *CEN01:1 Compatibility* requires one or more of Grönlund's (2003) policymaking stages to be digitized by the initiative system. Support congruence requires that systems of social support should be designed to reinforce the behaviors which the initiative is designed to elicit (Cherns, 1976, p. 790). Because compatibility requires the design process of an initiative to be compatible with the initiative's objectives, the initiative's support systems must also be compatible with the initiative's objectives.
	CEN02.3: Information gathering	E-Democratic Government seeks to increase civic participation through technology, and *CEN01:1 Compatibility* requires one or more of Grönlund's (2003) policymaking stages to be digitized by the initiative system. If an E-Democratic Government initiative does not allow participants to easily gather information from multiple sources, or does not enable the identification, organization, and filtering of information sources, the initiative system cannot be compatible with its objectives. This is because the policymaking process requires participants to have access to information deemed relevant by them to be considered successful. Without that information, discourse will ultimately displace outside of the initiative system, i.e., on social media.
	CEN02.4: Information retrieval and use	E-Democratic Government seeks to increase civic participation through technology, and *CEN01:1 Compatibility* requires one or more of Grönlund's (2003) policymaking stages to be digitized by the initiative system. If an E-Democratic Government initiative does not allow participants to easily retrieve, use, annotate, associate, or discuss information from multiple sources, the initiative system cannot be compatible with its objectives. This is because the policymaking process requires participants to have access to information deemed relevant by them to be considered successful. Without that information, discourse will ultimately displace outside of the initiative system, i.e., on social media.
	CEN02.5: Information sharing	E-Democratic Government seeks to increase civic participation through technology, and *CEN01:1 Compatibility* requires one or more of Grönlund's (2003) policymaking stages to be digitized by the initiative system. If an E-Democratic Government initiative does not support communal attitude, opinion, and choice formation through information sharing abilities defined by Robertson (2005), the initiative system cannot be compatible with its objectives. This is because the policymaking process requires participants to have access to information deemed relevant by them to be considered successful. Without that information, discourse will ultimately displace outside of the initiative system, i.e., on social media.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	CEN02.6: Trust, control, and information sources	E-Democratic Government seeks to increase civic participation through technology, and *CEN01:1 Compatibility* requires one or more of Grönlund's (2003) policymaking stages to be digitized by the initiative system. If an E-Democratic Government initiative does not protect participant identities, activities, or any other sensitive data that users define as private, the initiative system cannot be compatible with its objectives. This is because citizens will not meaningfully participate in the policymaking process, or participate in the fullest possible way, if they cannot define their information as private when they choose.
	SEC03: Disinformation Prevention	E-Democratic Government seeks to increase civic participation through technology, and *CEN01:1 Compatibility* requires one or more of Grönlund's (2003) policymaking stages to be digitized by the initiative system. If an E-Democratic Government initiative does not allow for the identification and removal of disinformation, the initiative system cannot be compatible with its objectives. This is because citizens will not meaningfully participate in the policymaking process, or participate in the fullest possible way, if they cannot decipher truth from falsehoods.
CEN01.2: Minimal critical specification	TGV02: Operational trust	If an E-Democratic Government initiative system has tasks, jobs, or roles that are more or less than what was originally specified, and citizens expect the digitization of policymaking stages, citizens will distrust the processes that deceived them.
	TGV03: Institutional trust	If an E-Democratic Government initiative system has tasks, jobs, or roles that are more or less than what was originally specified, and citizens expect the digitization of policymaking stages, citizens will distrust the institutions that deceived them.
	CEN01.9: Transitional organization	If transitions within an E-Democratic Government initiative system are not planned and designed before they occur, the initiative system can stray from tasks, jobs, and roles that were originally specified as a result, i.e., digitization of policymaking stages.
	CEN02.1: Integration of tasks	If an E-Democratic Government initiative system is not integrated into a single platform or is not accessible to users in this way, citizens may overlook some aspects of the disintegrated platform—effectively removing tasks, jobs, or roles that were originally specified.
	CEN02.2: Customization and personalization	If an E-Democratic Government initiative system does not allow participants to configure their own profiles, information filters, searches, and/or preferences, and the initiative system is designed for digitizing one or more of Grönlund's (2003) policymaking stages, the initiative system inherently has less tasks, jobs, and roles than were originally specified. This is because policymaking requires that citizens have access to relevant information when necessary, and without the ability to customize and personalize their information, such retrieval would be more difficult.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	CEN02.3: Information gathering	If an E-Democratic Government initiative system does not allow participants to gather information from multiple sources and identify, organize, and filter information sources, and the initiative system is designed for digitizing one or more of Grönlund's (2003) policymaking stages, the initiative system inherently has less tasks, jobs, and roles than were originally specified. This is because policymaking requires that citizens have access to relevant information when necessary, and without these abilities, such retrieval would be more difficult.
	CEN02.4: Information retrieval and use	If an E-Democratic Government initiative system does not allow participants to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others, and the initiative system is designed for digitizing one or more of Grönlund's (2003) policymaking stages, the initiative system inherently has less tasks, jobs, and roles than were originally specified. This is because policymaking requires that citizens have access to relevant information when necessary, and without these abilities, such retrieval would be more difficult.
	CEN02.5: Information sharing	If an E-Democratic Government initiative system does not support participants' abilities to form communal attitudes, opinions, and choices, and the initiative system is designed for digitizing one or more of Grönlund's (2003) policymaking stages, the initiative system inherently has less tasks, jobs, and roles than were originally specified. This is because policymaking requires that citizens can meaningfully deliberate, and without these abilities, such deliberation would be incomplete or more difficult.
	CEN02.7: Diversity of users	If an E-Democratic Government initiative system is not accessible to as many eligible citizens as possible, and the initiative system is designed for digitizing one or more of Grönlund's (2003) policymaking stages, the initiative system inherently has less tasks, jobs, and roles than were originally specified. This is because policymaking requires that citizens can meaningfully deliberate, and without meaningful representation of all (or most) eligible citizens, such deliberation would be incomplete.
CEN01.3: Variance control	All TGV requirements	*See TGV01—CEN01.3.*
	CEN01.9: Transitional organization	If an E-Democratic Government initiative system does not plan or design initiative transitions before they occur, the initiative system will inevitably import or export variances across bureaucratic or social boundaries. This is because planning and design give initiative administrators an opportunity to review transitions and their resistance against such importation and exportation. Without that opportunity, the chances of variances creeping in and out of the initiative system increase significantly.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	SEC02: Cybersecurity Maturity	Poor change management practices can indicate low cybersecurity maturity. Configuration change control processes are required to be in place, according to the NIST Cybersecurity Framework's Protect category and Information Protection Processes and Procedures subcategory (Barrett, 2018, p. 34).
CEN01.4: Boundary location	All TGV requirements	*See TGV01—CEN01.4.*
	CEN01.9: Transitional organization	If an E-Democratic Government initiative system does not plan or design initiative transitions before they occur, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because planning and design give initiative administrators an opportunity to review transitions and their resistance against such impediments. Without that opportunity, the chances of these impediments increase significantly. Further, these boundaries which cause impediments to the sharing of information, knowledge, and/or learning are typically drawn in a way that reflects bureaucratic and social boundaries (Alathur et al., 2011).
	CEN02.1: Integration of tasks	If an E-Democratic Government initiative system does not integrate tasks into one system, accessible to users in one place for a more seamless experience, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because citizens may overlook some aspects of the disintegrated platform—effectively introducing boundaries that impede sharing of information, knowledge, or learning.
	CEN02.2: Customization and personalization	If users of an E-Democratic Government initiative system do not have the abilities to configure their own information filters, searches, preferences, and profiles, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because policymaking requires that citizens have access to relevant information when necessary, and without the ability to customize and personalize their information, such retrieval would be more difficult. This introduces boundaries that impede sharing of information, knowledge, or learning.
	CEN02.3: Information gathering	If an E-Democratic Government initiative system does not allow participants to gather information from multiple sources and identify, organize, and filter information sources, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because policymaking requires that citizens have access to relevant information when necessary, and without these abilities, such retrieval would be more difficult. This introduces boundaries that impede sharing of information, knowledge, or learning.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	CEN02.4: Information retrieval and use	If an E-Democratic Government initiative system does not allow participants to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because policymaking requires that citizens have access to relevant information when necessary, and without these abilities, such retrieval would be more difficult. This introduces boundaries that impede sharing of information, knowledge, or learning.
	CEN02.5: Information sharing	If an E-Democratic Government initiative system does not support participants' abilities to form communal attitudes, opinions, and choices, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because policymaking requires that citizens can meaningfully deliberate, and without these abilities, such deliberation would be incomplete or more difficult. This introduces boundaries that impede sharing of information, knowledge, or learning.
	CEN02.7: Diversity of users	If an E-Democratic Government initiative system is not accessible to as many eligible citizens as possible, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning. This is because policymaking requires that citizens can meaningfully deliberate, and without meaningful representation of all (or most) eligible citizens, such deliberation would be incomplete. This introduces boundaries that impede sharing of information, knowledge, or learning.
	SEC01: Risk Management	If an E-Democratic Government initiative system does not have a comprehensive risk management program or allows one or more risks to compromise or exploit the initiative system, the initiative system will inevitably draw boundaries that impede sharing of information, knowledge, or learning due to its compromise or exploitation. This is because unmitigated risks can wreak havoc on people, processes, and technology.
CEN01.5: Information flow	All TGV requirements	*See TGV01—CEN01.5.*
	CEN01.6: Power and authority	If an E-Democratic Government initiative system does not properly administer power and authority or provide access to the resources required to administer power and authority, the initiative system cannot provide information to those who require it when they require it. This is because power and authority inherently require access control; without it, access cannot be accurately determined, and no one (or everyone) would have access to administrative resources.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	CEN02.2: Customization and personalization	If users of an E-Democratic Government initiative system do not have the abilities to configure their own information filters, searches, preferences, and profiles, the initiative system cannot provide information to those who require it when they require it.
	CEN02.3: Information gathering	If an E-Democratic Government initiative system does not allow participants to gather information from multiple sources and identify, organize, and filter information sources, the initiative system cannot provide information to those who require it when they require it.
	CEN02.4: Information retrieval and use	If an E-Democratic Government initiative system does not allow participants to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others, the initiative system cannot provide information to those who require it when they require it.
	CEN02.5: Information sharing	If an E-Democratic Government initiative system does not support participants' abilities to form communal attitudes, opinions, and choices, the initiative system cannot provide information to those who require it when they require it. This is because policymaking requires that citizens can meaningfully deliberate, and without these abilities, such deliberation would be incomplete or more difficult.
	SEC01: Risk Management	If an E-Democratic Government initiative system does not have a comprehensive risk management program or allows one or more risks to compromise or exploit the initiative system, the initiative system cannot provide information to those who require it when they require it. This is because unmitigated risks can wreak havoc on people, processes, and technology.
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative does not allow for the identification and removal of disinformation, the initiative system cannot provide information to those who require it when they require it. This is because policymaking requires that citizens can meaningfully deliberate, and without consensus on information's validity, such deliberation would be much more difficult.
CEN01.6: Power and authority	All TGV requirements	*See TGV01—CEN01.6.*
	CEN01.5: Information flow	*See CEN01.5—CEN01.6.*
	CEN02.4: Information retrieval and use	If an E-Democratic Government initiative system does not allow participants to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others, the system does not properly provide access to the resources required to administer power and authority. This is because policymaking requires that citizens have access to relevant information when necessary, and without these abilities, such retrieval would be more difficult.

E-Democratic Government Success Requirements	Internally Related Requirements	Description
	CEN02.6: Trust, control, and information sources	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, participants may blame elected power users for these shortcomings.
	CEN02.7: Diversity of users	If an E-Democratic Government initiative system is not accessible to as many eligible citizens as possible, the system does not properly provide access to the resources required to administer power and authority. This is because policymaking requires that citizens have access to relevant information when necessary, and without participation of as many citizens as possible, information will be incomplete.
	SEC01: Risk Management	Power and authority and risk management go hand in hand, as the concept of elected power users aligns with several NIST SP 800-53 controls, including AC-6 (least privilege), AU-10 (non-repudiation), and AC-5 (separation of duties) (NIST Joint Task Force, 2020, p. 36-103).
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative system does not allow for the identification and removal of disinformation by participants, elected power users could override designations of validity and allow disinformation to masquerade as truth.
	All PRV requirements	Elected power users have public visibility, and therefore will be part of sentiments relayed by citizens. For this reason, those with power roles must be accountable to these sentiments.
CEN01.7: Multifunctionality	TGV02: Operational trust	If an E-Democratic Government initiative system cannot add new roles or modify old ones, citizens will distrust the processes of the initiative system, as well as the institutions involved.
	TGV03: Institutional trust	*See CEN01.7—TGV02.*
	CEN01.10: Incompletion	If an E-Democratic Government initiative system cannot add new roles or modify old ones, incompletion, reassessment, and redesign of the initiative system are either impossible or much more difficult.
CEN01.8: Support congruence	TGV02: Operational trust	If the systems supporting an E-Democratic Government initiative system do not reinforce the behaviors which the initiative is designed to elicit, citizens will grow frustrated, confused, and eventually distrust the processes of the initiative system, as well as the institutions involved.
	TGV03: Institutional trust	*See CEN01.8—TGV02.*
	CEN01.1: Compatibility	*See CEN01.1—CEN01.8.*
	CEN02.3: Information gathering	If the systems supporting an E-Democratic Government initiative system do not reinforce the behaviors which the initiative is designed to elicit, participants are less likely to have the ability to effectively gather information.
CEN01.9: Transitional organization	TGV02: Operational trust	If an E-Democratic Government initiative system does not require planning and design of initiative transitions before they occur, transitions less likely to succeed and citizens will distrust the processes of the initiative system, as well as the institutions involved.
	TGV03: Institutional trust	*See CEN01.9—TGV02.*

E-Democratic Government Success Requirements	Internally Related Requirements	Description
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN01.9.*
	CEN01.3: Variance control	*See CEN01.3—CEN01.9.*
	CEN01.4: Boundary location	*See CEN01.4—CEN01.9.*
	SEC01: Risk Management	NIST SP 800-53's Configuration Management family provides controls for safeguarding information systems during transitions (NIST Joint Task Force, 2020, p. 437).
	SEC02: Cybersecurity Maturity	The NICE Framework (NIST SP 800-181)'s 'Information Protection Processes and Procedures' category within the Protect function map to NIST SP 800-53's Configuration Management family, *see CEN01.9—SEC01.*
CEN01.10: Incompletion	All TGV requirements	*See TGV01—CEN01.10.*
	CEN01.7: Multifunctionality	*See CEN01.7—CEN01.10.*
CEN02: Voter DSS Requirements per Robertson (2005)		
CEN02.1: Integration of tasks	TGV02: Operational trust	If an E-Democratic Government initiative system does not integrate tasks into one system, accessible to users in one place for a more seamless experience, citizens will distrust the processes of the initiative system, as well as the institutions involved.
	TGV03: Institutional trust	*See CEN02.1—TGV02.*
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN02.1.*
	CEN01.4: Boundary location	*See CEN01.4—CEN02.1.*
	CEN02.3: Information gathering	If an E-Democratic Government initiative system does not integrate tasks into one system, accessible to users in one place for a more seamless experience, participants' abilities to gather information from multiple sources and identify, organize, and filter information sources are severely hampered through obscurity.
	CEN02.4: Information retrieval and use	If an E-Democratic Government initiative system does not integrate tasks into one system, it hampers participants' ability to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others.
	CEN02.5: Information sharing	If an E-Democratic Government initiative system does not integrate tasks into one system, the initiative system does not support participants' abilities to form communal attitudes, opinions, and choices through obscurity.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	CEN02.6: Trust, control, and information sources	If an E-Democratic Government initiative system does not integrate tasks into one system, the initiative cannot comprehensively protect participants' identities and relevant participation information that they define as private.
	CEN02.7: Diversity of users	If an E-Democratic Government initiative system does not integrate tasks into one system, the complexity of the platform may drive away those who are less familiar with technology. The consequence would be an incomplete picture of citizen sentiments.
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative system does not integrate tasks into one system, the identification and removal of disinformation would become much more difficult, if not impossible.
CEN02.2: Customization and personalization	TGV02: Operational trust	If users of an E-Democratic Government initiative system do not have the abilities to configure their own information filters, searches, preferences, and profiles, citizens will distrust the processes of the initiative system, as well as the institutions involved.
	TGV03: Institutional trust	*See CEN02.2—TGV02.*
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN02.2.*
	CEN01.4: Boundary location	*See CEN01.4—CEN02.2.*
	CEN01.5: Information flow	*See CEN01.5—CEN02.2.*
	CEN02.3: Information gathering	If users of an E-Democratic Government initiative system cannot customize and personalize their information filters, searches, preferences, and profiles, participants' abilities to gather information from multiple sources and identify, organize, and filter information sources are severely hampered through obscurity.
	CEN02.4: Information retrieval and use	If users of an E-Democratic Government initiative system cannot customize and personalize their information filters, searches, preferences, and profiles, it hampers participants' ability to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others.
	CEN02.5: Information sharing	If users of an E-Democratic Government initiative system cannot customize and personalize their information filters, searches, preferences, and profiles, the initiative system does not support participants' abilities to form communal attitudes, opinions, and choices.
	CEN02.6: Trust, control, and information sources	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, the initiative system cannot honestly and accurately customize and personalize their information filters, searches, preferences, and profiles.

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	SEC03: Disinformation Prevention	If users of an E-Democratic Government initiative system cannot customize and personalize their information filters, searches, preferences, and profiles, the identification and removal of disinformation is still possible but much more difficult, both practically and in terms of managing the resulting perception.
CEN02.3: Information gathering	All TGV requirements	*See TGV01—CEN02.3.*
	CEN01.1: Compatibility	*See CEN01.1—CEN02.3.*
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN02.3.*
	CEN01.4: Boundary location	*See CEN01.4—CEN02.3.*
	CEN01.5: Information flow	*See CEN01.5—CEN02.3.*
	CEN01.8: Support congruence	*See CEN01.8—CEN02.3.*
	CEN02.1: Integration of tasks	*See CEN02.1—CEN02.3.*
	CEN02.2: Customization and personalization	*See CEN02.2—CEN02.3.*
	CEN02.5: Information sharing	If an E-Democratic Government initiative system does not support participants' abilities to form communal attitudes, opinions, and choices, participants' ability to gather information from multiple sources and identify, organize, and filter information sources are severely hampered.
	CEN02.6: Trust, control, and information sources	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, participants' ability to gather information from multiple sources and identify, organize, and filter information sources are severely hampered through lowered expectation of privacy and violations of privacy.
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative does not allow for the identification and removal of disinformation, participants' ability to gather information from multiple sources and identify, organize, and filter information sources are severely hampered due to uncertainty of information's validity.
CEN02.4: Information retrieval and use	TGV02: Operational trust	If an E-Democratic Government initiative system does not allow participants to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others, citizens will distrust the processes of the initiative system, as well as the institutions involved.
	TGV03: Institutional trust	*See CEN02.4—TGV02.*
	CEN01.1: Compatibility	*See CEN01.1—CEN02.4.*
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN02.4.*

E-Democratic Government Success Requirements	Internally Related Requirements	Description
	CEN01.4: Boundary location	*See CEN01.4—CEN02.4.*
	CEN01.5: Information flow	*See CEN01.5—CEN02.4.*
	CEN01.6: Power and authority	*See CEN01.6—CEN02.4.*
	CEN02.1: Integration of tasks	*See CEN02.1—CEN02.4.*
	CEN02.2: Customization and personalization	*See CEN02.2—CEN02.4.*
	CEN02.5: Information sharing	If an E-Democratic Government initiative system does not support participants' abilities to form communal attitudes, opinions, and choices, it hampers participants' ability to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others.
	CEN02.6: Trust, control, and information sources	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, it hampers participants' ability to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others.
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative does not allow for the identification and removal of disinformation, it hampers participants' ability to use retrieval, organizational, and existing Internet search tools, or allow them to annotate, discuss, interact with, and associate information with others.
CEN02.5: Information sharing	All TGV requirements	*See TGV01—CEN02.5.*
	CEN01.1: Compatibility	*See CEN01.1—CEN02.5.*
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN02.5.*
	CEN01.4: Boundary location	*See CEN01.4—CEN02.5.*
	CEN01.5: Information flow	*See CEN01.5—CEN02.5.*
	CEN02.1: Integration of tasks	*See CEN02.1—CEN02.5.*
	CEN02.2: Customization and personalization	*See CEN02.2—CEN02.5.*
	CEN02.4: Information retrieval and use	*See CEN02.4—CEN02.5.*
	CEN02.6: Trust, control, and information sources	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, the initiative system does not support participants' abilities to form communal attitudes, opinions, and choices.
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative does not allow for the identification and removal of disinformation,

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	All PRV requirements	If the initiative system does not support communal attitude, opinion, and choice formation through information sharing abilities, the citizens will eventually distrust the privacy of their activities and data within the initiative system.
CEN02.6: Trust, control, and information sources	All TGV requirements	*See TGV01—CEN02.6.*
	CEN01.1: Compatibility	*See CEN01.1—CEN02.6.*
	CEN01.6: Power and authority	*See CEN01.6—CEN02.6.*
	CEN02.1: Integration of tasks	*See CEN02.1—CEN02.6.*
	CEN02.2: Customization and personalization	*See CEN02.2—CEN02.6.*
	CEN02.3: Information gathering	*See CEN02.3—CEN02.6.*
	CEN02.4: Information retrieval and use	*See CEN02.4—CEN02.6.*
	CEN02.5: Information sharing	*See CEN02.5—CEN02.6.*
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, the identification and removal of disinformation becomes much less trustworthy to participants.
	All PRV requirements	If an E-Democratic Government initiative system does not protect participants' identities and relevant participation information that they define as private or selects and categorizes information sources in a biased way, the citizens will eventually distrust the privacy of their activities and data within the initiative system.
CEN02.7: Diversity of users	All TGV requirements	*See TGV01—CEN02.7.*
	CEN01.2: Minimal critical specification	*See CEN01.2—CEN02.7.*
	CEN01.4: Boundary location	*See CEN01.4—CEN02.7.*
	CEN01.6: Power and authority	*See CEN01.6—CEN02.7.*
	CEN02.1: Integration of tasks	*See CEN02.1—CEN02.7.*
	SEC03: Disinformation Prevention	If an E-Democratic Government initiative excludes certain groups of citizens, regardless of by how those groups are determined, the resulting identification and removal of disinformation could be viewed as discriminatory against those groups, or incomplete at minimum.
Security (SEC)		
SEC01: Risk Management	All TGV requirements	Risk management is necessary for maintaining and increasing trust in government. If the initiative system was compromised and data was changed or stolen due to poor risk management, citizens would distrust the people, processes, and institutions which did not defend their data.

E-Democratic Government Success Requirements	Internally Related Requirements	Description
	CEN01.4: Boundary location	*See CEN01.4—SEC01.*
	CEN01.5: Information flow	*See CEN01.5—SEC01.*
	CEN01.6: Power and authority	*See CEN01.6—SEC01.*
	CEN01.9: Transitional organization	*See CEN01.9—SEC01.*
	SEC02: Cybersecurity Maturity	NIST SP 800-53 controls and NICE Framework (NIST SP 800-181) categories are mapped to each other in the latter publication (Barrett, 2018; NIST Joint Task Force, 2020).
	All PRV requirements	If the initiative system was compromised and data was changed or stolen due to poor risk management, the citizens will eventually distrust the privacy of their activities and data within the initiative system.
SEC02: Cybersecurity Maturity	All TGV requirements	Cybersecurity maturity is necessary for maintaining and increasing trust in government. If the initiative system was compromised and data was changed or stolen due to insufficient cybersecurity maturity, citizens would distrust the people, processes, and institutions which did not defend their data.
	CEN01.3: Variance control	*See CEN01.3—SEC02.*
	CEN01.9: Transitional organization	*See CEN01.9—SEC02.*
	SEC01: Risk Management	*See SEC01—SEC02.*
	All PRV requirements	If the initiative system was compromised and data was changed or stolen due to insufficient cybersecurity maturity, the citizens will eventually distrust the privacy of their activities and data within the initiative system.
SEC03: Disinformation Prevention	All TGV requirements	Disinformation prevention is necessary for maintaining and increasing trust in government. If the initiative system has no means to remove disinformation, citizens will no longer trust the people, processes, and institutions that built the system if it is perceived to be overcome with falsehoods.
	CEN01.1: Compatibility	*See CEN01.1—SEC03.*
	CEN01.5: Information flow	*See CEN01.5—SEC03.*
	CEN01.6: Power and authority	*See CEN01.6—SEC03.*
	All CEN02 requirements	*See CEN02.1-7—SEC03.*
Privacy (PRV) per Gerber et al. (2018)	All TGV requirements	*See TGV01—All PRV requirements.*
	CEN01.6: Power and authority	*See CEN01.6—All PRV requirements.*
	CEN02.5: Information sharing	*See CEN02.5—All PRV requirements.*
	CEN02.6: Trust, control, and information sources	*See CEN02.6—All PRV requirements.*
	SEC01: Risk Management	*See SEC01—All PRV requirements.*

E-Democratic Government Success Requirements	**Internally Related Requirements**	**Description**
	SEC02: Cybersecurity Maturity	*See SEC02—All PRV requirements.*
PRV01: Privacy attitude, concerns, and perceived risk		
PRV02: Privacy-related behavioral intention and willingness		
PRV03: Information disclosure behavior		
PRV04: Protection behavior and privacy settings		

CHAPTER 6

CONCLUSIONS

Citizens' civic engagement in US municipal politics has diminished over the last few decades in both quantity and quality, and the causes and effects of this decrease offer some explanations for why the US has not yet meaningfully used technology to enhance the government-to-citizen relationship. First, social capital has eroded in the past fifty years due to suburbanization, commuting, sprawl, pressures of time and money, generational change, and the effect of electronic entertainment—especially the last two (Putnam, 2001). Social capital, or relationships of trust and reciprocity among citizens, is crucial for maintaining robust, effective democracies. This erosion accelerated during the COVID-19 pandemic, as US municipal political bodies (mostly operated through non-technological means like town halls and in-person meetings) adopted technologies they had never used before to conduct political business. Predictably, the effects of social capital erosion appear to have further ostracized those most marginalized (Leighley & Nagler, 2013). Second, the state of E-Democracy in the US is remarkably poor. US States and localities have found a little more success than has the US Federal Government, but even with municipal initiatives like *Boston311* and *NYC311*, these initiatives have not yet created or expanded government services that do not have a nontechnological equivalent. In other words, E-Democracy in the US has been more focused on efficiency rather than truly enhancing the government-to-citizen relationship. Finally, related research areas that could inform and improve E-Democratic Government success were identified, analyzed, and included as necessary: decision support systems (machine learning and text mining supporting governmental analytics and citizen learning), cybersecurity, privacy, trust in government, citizen engagement through design, and citizen engagement as a metric of success.

To address the problem of low citizen engagement in US municipal politics, this dissertation offers a framework (method) artifact that provides guidance informing the success of the requirements, design, implementation, adoption, and evaluation of E-Democratic Government initiatives. Borrowing from the E-Democracy and E-Government literature, I developed the hybrid conception of E-Democratic Government to emphasize that my framework not only seeks to deliver government information by digital means, but that it also aims to increase citizen engagement in civic, deliberative, and political activity.

As a starting point, I conducted an evaluation of this artifact using benchmarking through a comparative gap analysis of the artifact. For this analysis, I examined past and current US E-Democracy initiatives and found no existing evidence that they had increased civic engagement. Federal US E-Democracy initiatives had little to do with policymaking and were largely self-serving, whereas State US E-Democracy initiatives invoked more bilateral communication between citizens and government through 311 platforms yet were under-resourced and often lost sight of the normative purpose of increasing civic engagement. From this startling finding, I concluded that these initiatives failed to meet the basic requirements of my framework for E-Democratic Government.

Next, I mapped six prominent cybersecurity frameworks and theories to relevant requirements of my framework, but I found, like in the benchmarking analysis, that most of the existing cybersecurity frameworks fell short of the standards I had set for developing E-Democratic strategies. Perhaps this shortcoming stems from the organizational governance focus that cybersecurity frameworks and theories prioritize over democratic governance, as I was only able to identify seven connections to cybersecurity frameworks and theories out of 38 individual requirements. I then turned to developing a synthetic lawsourcing scenario. My goal here was to better communicate the framework's requirements to practitioners and other users of the framework. Although the lack of literature hindered the application of some of the framework's requirements, I found enough literature and scenario creation examples to inform my application of the remainder of the framework's requirements. This suggests that users should be able to gain further insights into the spirit of the framework using this evaluation. Finally, regarding the application of defense in depth, I identified 94 total connections among the framework's five major categories and 38 individual requirements. The goal of this evaluation technique was to strengthen the validity of the artifact, and that goal was accomplished by demonstrating the interrelatedness of the framework's requirements.

This project offers important contributions to knowledge and practice. Regarding knowledge, I completed a literature review and analysis in many research areas that relate to the use of technology to increase civic engagement, including E-Government, E-Democracy, deliberative democracy, decision support systems, computer security, user privacy, trust in government, and citizen engagement. As noted above, the literature analysis encouraged me to propose a new hybrid term, E-Democratic Government, since I found existing terms in the literature, notably E-Democracy and E-Government, either contested or ambiguous. When I determined which research areas to use for developing E-Democratic Government strategies and their application through the framework artifact, I considered the appropriateness of each research area's inclusion in the sixth design science research step, known as design as a search process—especially when there were multiple distinct, yet closely-related research areas (Hevner et al., 2004). For example, sociotechnical theory is very closely related to participatory theory, as each research area pursues increased engagement through design of technology. I used sociotechnical theory to inform the recommendations on citizen engagement through design because of differences in published literature between sociotechnical theory and participatory theory. The participatory theory literature that I considered for this research consisted mostly of case studies in K-12 classrooms, whereas gathered sociotechnical theory literature included case studies that designed many different technologies in many different environments—some of which were closer to E-Democratic Government than a K-12 classroom.

Another important contribution I make in this project concerns the methodological approach taken with the artifact's evaluation. Without previous experiments in E-Democratic Government or a willing participating government to conduct a pilot project, I faced a major challenge in developing a sufficient evaluation strategy for my E-Democratic Government framework. However, I used multiple descriptive evaluation techniques to strengthen an otherwise limited evaluation category, and my approach here could be used in future design science research projects, especially ones with little to no available resources.

Regarding contributions to practice, the artifact framework is a versatile tool that can be used by three distinct and broad populations: public government officials and/or employees in United States' municipalities, citizens and/or third parties, and researchers interested in E-Democratic Government or related fields. For the first use case, practitioners can use the framework artifact to start, design, manage, and/or evaluate E-Democratic Government initiatives. For the second use case, citizens and/or third parties can use the framework artifact to evaluate or propose E-Democratic Government initiatives. Finally, researchers studying the integration of information communication technologies into the policymaking process (and other related fields) can use the framework artifact as a research agenda to further work in one or more of the many included research areas.

Although this research would be considered ambitious to some, it has a few important limitations. First and most importantly, no real-world test was conducted on the artifact, as this research aimed only to provide a framework of guidance informing the success of E-Democratic Government initiatives. Even though many governmental and peer-reviewed, academic publications were referenced and connected to each of the framework's requirements, and many of those publications include real-world experiments, one or more pilot studies with willing and authorized US municipal governments should be conducted to assess and improve this framework's utility.

Second, the framework is complex considering its five major requirements and 38 individual requirements, and this complexity may cause users to misunderstand or misinterpret aspects of the framework or steer them away from adoption entirely. However, this research project demonstrates that E-Democratic Government is unavoidably complex, and the artifact already simplifies many success requirements into five major categories. Further, the lawsourcing scenario in Table 5.3 provides guidance to new framework users by demonstrating the application of each framework success requirement. Of course, the alternative to the ambitious and complex strategies offered here is the largely unacceptable status quo: declining social capital, rampant disinformation, and the further infusion of technology into democracy and politics with no normative purpose (aside from giving existing influential political actors even greater influence in shaping political and policy outcomes).

Finally, some areas within the provided framework guidance may be missing, incomplete, overly detailed, or insufficiently detailed. Some connections made in this work may not play out the same way in every instance, and some of the decisions made in the design of this framework may turn out to be incorrect or flawed. I also expect that some areas will need to be added, removed, or modified over time. In part, this is due to the first limitation. Real-world testing may reveal some discrepancies that my review and analysis of the literature did not. For example, concerning the digital divide and the limited technological abilities of users, the only recommendation I found in the literature came from Robertson (2005), who suggests that public-use kiosk stations available at libraries and cafes could help to bridge the economic digital divide. By extension, support staff who are typically available at public-use kiosk stations could assist those with insufficient technological abilities. Although this is not an especially sophisticated solution, the question of the most effective means to include users with insufficient technological abilities in a digital network is one that was not explicitly addressed in this work. Accordingly, this research gathered and used recommendations from research on similar contested or outstanding micro issues and left final determinations for these areas to future work. In the case of the digital divide, future work should test and evaluate different methods of including users with insufficient technological abilities in a digital network through real-world experiments. Lastly, the nature of the human condition plays a role in this limitation—after all, nothing and no one is perfect.

For future research, one pilot study or more should be conducted by implementing the framework artifact through a willing and authorized US municipal government. Pre-testing and post-testing of citizen sentiments, civic engagement, legislative activity, and any other relevant metrics should be conducted and analyzed to assess the framework's impact. Further, qualitative case study or ethnographic research could be conducted alongside such a pilot study to gain more insights into an initiative's success or lack thereof. Regarding the different subject matters within the framework, each has much room for improvement. For example, sociotechnical theory—the driving principles behind this framework's citizen engagement through design—already has an established research domain, along with many other subject matters. Decision support systems, often supported by machine learning, are likely to dramatically improve and expand in use soon due to the rapid advances in machine learning and artificial intelligence. Finally, although the cybersecurity landscape is continually changing, there is a significant lack of research in preventing disinformation—let alone preventing disinformation in a governmental platform. This problem concerns both political science and information security disciplines, and this research suggests that preventing some categories of disinformation should be addressed by the communities through the systematic identification of, consensus about, and removal of disinformation.

In closing, by creating and evaluating this framework, I intend to eventually increase the prevalence and success of E-Democracy initiatives in US municipal politics. This work is just a beginning; whether that goal will be met largely depends on publications that grow out of this dissertation, and the attention that those publications may or may not receive (aside from my footwork of finding a willing and authorized US municipal government for pilot testing). This goal equally depends on how passionate US citizens and their local governments are about democracy and, in particular, repairing and enhancing the government-to-citizen relationship. The success of democracy, and any integration of technology into it, is up to the US population.

REFERENCES

Agawu, E. (2017). *What's Next for E-Government? Innovations in E-Government Through a Cybersecurity Lens*.

Aladwani, A. M., & Dwivedi, Y. K. (2018, 2018/12/01/). Towards a theory of SocioCitizenry: Quality anticipation, trust configuration, and approved adaptation of governmental social media. *International Journal of Information Management, 43*, 261-272. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.08.009

Alathur, S., Ilavarasan, P. V., & Gupta, M. P. (2011). *Citizen empowerment and participation in e-democracy: Indian context* Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, Tallinn, Estonia.

Alford, R. R., & Lee, E. C. (1968). Voting Turnout in American Cities. *The American Political Science Review, 62*(3), 796-813. https://doi.org/10.2307/1953431

AlSuwaidi, M. A., & Rajan, A. V. (2013, 11-12 Dec. 2013). E-government failure and Success Factors Rank Model an extension of Heeks Factor Model. 2013 International Conference on Current Trends in Information Technology (CTIT),

Altameem, T., Zairi, M., & Alshawi, S. (2006, 19-21 Nov. 2006). Critical Success Factors of E-Government: A Proposed Model for E-Government Implementation. 2006 Innovations in Information Technology,

Andrews, B., & Pruysers, S. (2022). Does Democracy Die in Darkness? An Examination of the Relationship between Local Newspaper Health and Turnout in Municipal Politics. *Canadian Journal of Political Science*, 1-14. https://doi.org/10.1017/S0008423922000737

Antoni, D., Bidar, A., Herdiansyah, M. I., & Akbar, M. (2017, 1-3 Nov. 2017). Critical factors of transparency and trust for evaluating e-government services for the poor. 2017 Second International Conference on Informatics and Computing (ICIC), Avgerou, C. (2013). Explaining Trust in IT-Mediated Elections: A Case Study of E-Voting in Brazil [Case Study]. *14*, 420-451. http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=92571027&site=ehost-live&scope=site

Ayyad, M. (2017). *How Does e-Government Work?* Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance, New Delhi AA, India.

Bächtiger, A. (2018). *The Oxford Handbook of Deliberative Democracy*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198747369.001.0001

Banjak-Corle, C., & Wallace, L. N. (2021, 2021/01/15). Disaster experiences and terrorism news exposure: effects on perceptions of police and trust in local government in the United States. *Police Practice and Research, 22*(1), 542-556. https://doi.org/10.1080/15614263.2020.1716356

Barrett, M. P. (2018, January 27, 2020). *Framework for Improving Critical Infrastructure Cybersecurity*. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Bateman, P. J., Gray, P. H., & Butler, B. S. (2011). The Impact of Community Commitment on Participation in Online Communities [Article]. *Information Systems Research, 22*(4), 841-854. https://doi.org/10.1287/isre.1090.0265

Batlle-Montserrat, J., Blat, J., & Abadal, E. (2014). Benchmarking Municipal E-Government Services: A Bottom-Up Methodology and Pilot Results. *International Journal of Electronic Government Research (IJEGR), 10*(4), 57-75. https://doi.org/10.4018/ijegr.2014100103

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4-17. https://doi.org/10.1016/j.intcom.2010.07.003

Bell, D. E., & La Padula, L. J. (1976). *Secure Computer System: Unified Exposition and Multics Interpretation*. http://dx.doi.org/10.21236/ada023588

Bonacin, R., Melo, A. M., Simoni, C. A., & Baranauskas, M. C. (2010, Mar 20102011-10-26). Accessibility and interoperability in e-government systems: outlining an inclusive development process. *Universal Access in the Information Society, 9*(1), 17-33. https://doi.org/http://dx.doi.org/10.1007/s10209-009-0157-0

Bridges, A. (1999). *Morning glories: Municipal reform in the Southwest*. Princeton University Press.

Calderon, N. A., Fisher, B., Hemsley, J., Ceskavich, B., Jansen, G., Marciano, R., & Lemieux, V. L. (2015, 29 Oct.-1 Nov. 2015). Mixed-initiative social media analytics at the World Bank: Observations of citizen sentiment in Twitter data to explore "trust" of political actors and state institutions and its relationship to social protest. 2015 IEEE International Conference on Big Data (Big Data)

Carvalho, G., Souza, J. M., & Medeiros, S. P. J. (2009, 22-24 April 2009). Collaboration engineering, philosophy, and Democracy with LaSca. 2009 13th International Conference on Computer Supported Cooperative Work in Design

Cassini, J. A., Medlin, B. D., & Adriana, R. (2008). Laws and Regulations Dealing with Information Security and Privacy: An Investigative Study. *International Journal of Information Security and Privacy (IJISP), 2*(2), 70-82. https://doi.org/10.4018/jisp.2008040105

Charalabidis, Y., Loutsaris, M. A., Virkar, S., Alexopoulos, C., Novak, A.-S., & Lachana, Z. (2019). *Use Case Scenarios on Legal Text Mining* Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, Melbourne, VIC, Australia.

Cherns, A. (1976). The Principles of Sociotechnical Design. *Human Relations, 29*(8), 783-792. https://doi.org/10.1177/001872677602900806

Cherns, A. (1987). Principles of Sociotechnical Design Revisted. *Human Relations, 40*(3), 153-161. https://doi.org/10.1177/001872678704000303

Chugunov, A., Filatova, O., & Misnikov, Y. (2016). *Online Discourse as a Microdemocracy Tool: Towards New Discursive Epistemics for Policy Deliberation* Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance, Montevideo, Uruguay.

Clegg, C. W. (2000, 2000/10/02/). Sociotechnical principles for system design. *Applied Ergonomics, 31*(5), 463-477. https://doi.org/https://doi.org/10.1016/S0003-6870(00)00009-0

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease Of Use, And User Accep. *MIS Quarterly, 13*(3), 319.

Farrell, H. J., & Schneier, B. (October 2018). Common-Knowledge Attacks on Democracy. *Berkman Klein Center Research Publication, 2018-7*. https://ssrn.com/abstract=3273111

Farris, E. M., & Holman, M. R. (2023, 2023/02/22). Sheriffs, right-wing extremism, and the limits of U.S. federalism during a crisis [https://doi.org/10.1111/ssqu.13244]. *Social Science Quarterly, n/a*(n/a). https://doi.org/https://doi.org/10.1111/ssqu.13244

Federal Financial Institutions Examination Council (2017, May 2017). *FFIEC Cybersecurity Assessment Tool*. Retrieved 10/14 from https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf

Fraser, M. D., & Vaishnavi, V. K. (1997, 1997/12//). A formal specifications maturity model. *Communications of the ACM*, *40*(12), 95+. https://link.gale.com/apps/doc/A20447660/AONE?u=nysl_we_niagarau&sid=AONE&xid=8f226c88

Fu, Q., Feng, B., Guo, D., & Li, Q. (2018, 2018/01/01/). Combating the evolving spammers in online social networks. *Computers & Security, 72*(Supplement C), 60-73. https://doi.org/https://doi.org/10.1016/j.cose.2017.08.014

Gerber, M., & von Solms, R. (2008, 2008/10/01/). Information security requirements – Interpreting the legal aspects. *Computers & Security, 27*(5), 124-135. https://doi.org/https://doi.org/10.1016/j.cose.2008.07.009

Gerber, N., Gerber, P., & Volkamer, M. (2018, 2018/08/01/). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226-261. https://doi.org/https://doi.org/10.1016/j.cose.2018.04.002

Germonprez, M., Kendall, J. E., Kendall, K. E., Mathiassen, L., Young, B., & Warner, B. (2017). A Theory of Responsive Design: A Field Study of Corporate Engagement with Open Source Communities. *Information Systems Research, 28*(1), 64-83.

Gil-Garcia, J. R., & Flores-Zúñiga, M. Á. (2020, 2020/10/01/). Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. *Government Information Quarterly, 37*(4), 101518. https://doi.org/https://doi.org/10.1016/j.giq.2020.101518

Gil-Garcia, J. R., & Martinez-Moyano, I. J. (2007, 2007/04/01/). Understanding the evolution of e-government: The influence of systems of rules on public sector dynamics. *Government Information Quarterly, 24*(2), 266-290. https://doi.org/https://doi.org/10.1016/j.giq.2006.04.005

Groat, S., Tront, J., & Marchany, R. (2012, 16-19 July 2012). Advancing the defense in depth model. 2012 7th International Conference on System of Systems Engineering (SoSE), Grönlund, Å. (2003, Mar-Jun, 2012-02-07). e-democracy: in search of tools and methods for effective participation. *Journal of Multicriteria Decision Analysis, 12*(2-3), 93-93+. http://www.ezproxy.dsu.edu:2048/login?url=https://search.proquest.com/docview/215211912?accountid=27073

Grumbach, J. (2022). *Laboratories Against Democracy : How National Parties Transformed State Politics*. Princeton University Press. http://ebookcentral.proquest.com/lib/niagara-ebooks/detail.action?docID=6985936

Hahanov, V., Litvinova, E., Brazhnikova, M., & Hahanova, A. (2016, 23-26 Feb. 2016). Cyber democracy and digital relationship. 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET),

Hajnal, Z. L., & Lewis, P. G. (2003). Municipal Institutions and Voter Turnout in Local Elections. *Urban Affairs Review, 38*(5), 645-668. https://doi.org/10.1177/1078087403038005002

Hanson, S., Jiang, L., & Dahl, D. (2019, 2019/03/01). Enhancing consumer engagement in an online brand community via user reputation signals: a multi-method analysis. *Journal of the Academy of Marketing Science, 47*(2), 349-367. https://doi.org/10.1007/s11747-018-0617-2

Hansson, K., Karlström, P., Larsson, A., & Verhagen, H. (2014, Jun 20142014-08-31). Reputation, inequality and meeting techniques: visualising user hierarchy to support collaboration. *Computational and Mathematical Organization Theory, 20*(2), 155-175. https://doi.org/http://dx.doi.org/10.1007/s10588-013-9165-y

Hapsara, M. (2016, 9-11 May 2016). Reinstating e-voting as a socio-technical system: A critical review of the current development in developing countries. 2016 IEEE Region 10 Symposium (TENSYMP), Heaton, B. (2015). *California Assemblyman Mike Gatto Talks Data Security, Tech Education*. Retrieved August 4 from https://www.govtech.com/state/California-Assemblyman-Mike-Gatto-Talks-Data-Security-Tech-Education.html

Hevner, A., March, S., Park, J., & Ram, S. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH 1. *MIS Quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625

Holbrook, T. M., & Weinschenk, A. C. (2019, 2020/03/01). Information, Political Bias, and Public Perceptions of Local Conditions in U.S. Cities. *Political Research Quarterly, 73*(1), 221-236. https://doi.org/10.1177/1065912919892627

Hossan, C. G., & Ryan, J. C. (2018). Factors Affecting E-Government Technology Adoption Behaviour in a Voluntary Environment. In *Technology Adoption and Social Issues: Concepts, Methodologies, Tools, and Applications* (pp. 447-475). IGI Global. https://doi.org/10.4018/978-1-5225-5201-7.ch020

Jaidka, K., & Ahmed, S. (2015). *The 2014 Indian general election on Twitter: an analysis of changing political traditions* Proceedings of the Seventh International Conference on Information and Communication Technologies and Development, Singapore, Singapore.

Jamal, A., Keohane, R., Romney, D., & Tingley, D. (2015). Anti-Americanism and Anti-Interventionism in Arabic Twitter Discourses. *Perspectives on Politics, 13*(1), 55-73. https://doi.org/10.1017/S1537592714003132

Katakis, I., Tsapatsoulis, N., Mendez, F., Triga, V., & Djouvas, C. (2014). Social Voting Advice Applications—Definitions, Challenges, Datasets and Evaluation. *IEEE Transactions on Cybernetics, 44*(7), 1039-1052. https://doi.org/10.1109/TCYB.2013.2279019

Kersting, N. (2012). The Future of Electronic democracy. In N. Kersting, M. Stein, & J. Trent (Eds.), *Electronic Democracy* (1 ed., pp. 11-54). Verlag Barbara Budrich. https://doi.org/10.2307/j.ctvddzwcg.5

Kouba, K., Novák, J., & Strnad, M. (2021, 2021/01/01). Explaining voter turnout in local elections: a global comparative perspective. *Contemporary Politics, 27*(1), 58-78. https://doi.org/10.1080/13569775.2020.1831764

Kulkarni, U. R., Ravindran, S., & Freeze, R. (2006, Winter2006/2007). A Knowledge Management Success Model: Theoretical Development and Empirical Validation [Article]. *Journal of Management Information Systems, 23*(3), 309-347. http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=23726558&site=ehost-live&scope=site

Lappas, G., Triantafillidou, A., Kleftodimos, A., & Yannas, P. (2015, 24-26 Aug. 2015). Evaluation framework of local e-government and e-democracy: A citizens' perspective. 2015 IEEE Conference on e-Learning, e-Management and e-Services (IC3e),

Leighley, J. E., & Nagler, J. (2013). *Who Votes Now? : Demographics, Issues, Inequality, and Turnout in the United States*. Princeton University Press. http://ebookcentral.proquest.com/lib/niagara-ebooks/detail.action?docID=1458379

Lidén, G. (2013). Supply of and demand for e-democracy: A study of the Swedish case [Article]. *Information Polity: The International Journal of Government & Democracy in the Information Age, 18*(3), 217-232. https://doi.org/10.3233/IP-130308

Lin, Y. (2018, Nov 2018, 2019-01-23). A comparison of selected Western and Chinese smart governance: The application of ICT in governmental management, participation and collaboration. *Telecommunications Policy, 42*(10), 800. https://doi.org/http://dx.doi.org/10.1016/j.telpol.2018.07.003

Liu, C., Zhang, Y., Li, Z., Zhang, J., Qin, H., & Zeng, J. (2015, 19-20 Dec. 2015). Dynamic Defense Architecture for the Security of the Internet of Things. 2015 11th International Conference on Computational Intelligence and Security (CIS),

Liu, Y., & Zhou, C. (2010, 16-18 July 2010). A citizen trust model for e-government. 2010 IEEE International Conference on Software Engineering and Service Sciences,

Lyytinen, K., & Newman, M. (2008, Dec 2008, 2018-10-06). Explaining information systems change: a punctuated socio-technical change model. *European Journal of Information Systems, 17*(6), 589-613. https://doi.org/http://dx.doi.org/10.1057/ejis.2008.50

Marques, M. R. S., Bianco, T., Roodnejad, M., Baduel, T., & Berrou, C. (2019). *Machine learning for explaining and ranking the most influential matters of law* Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law, Montreal, QC, Canada.

McCumber, J. (2004). *Assessing and Managing Security Risk in IT Systems*. Auerbach Publications. https://doi.org/10.1201/9780203490426

Mell, P., Shook, J., & Harang, R. (2016). *Measuring and Improving the Effectiveness of Defense-in-Depth Postures* Proceedings of the 2nd Annual Industrial Control System Security Workshop, Los Angeles, CA, USA.

Mergel, I. (2010). The Use of Social Media to Dissolve Knowledge Silos in Government. In R. O'Leary, D. M. Van Slyke, & S. Kim (Eds.), *The Future of Public Administration around the World* (pp. 177-184). Georgetown University Press. http://www.jstor.org.ezproxy.niagara.edu/stable/j.ctt2tt4cr.26

Miron, W., & Muita, K. (2014, Oct 2014, 2014-12-19). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review, 4*(10), 33-39. http://www.ezproxy.dsu.edu:2048/login?url=https://search.proquest.com/docview/1638205900?accountid=27073

Morlan, R. L. (1984). Municipal vs. National Election Voter Turnout: Europe and the United States. *Political Science Quarterly, 99*(3), 457-470. https://doi.org/10.2307/2149943

Mossberger, K., Wu, Y., & Crawford, J. (2013, 2013/10/01/). Connecting citizens and local governments? Social media and interactivity in major U.S. cities. *Government Information Quarterly, 30*(4), 351-358. https://doi.org/https://doi.org/10.1016/j.giq.2013.05.016

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus, 140*(4), 70-92. www.jstor.org/stable/23046915

Naicker, V., & Mafaiti, M. (2019, 2019/01/01/). The establishment of collaboration in managing information security through multisourcing. *Computers & Security, 80*, 224-237. https://doi.org/https://doi.org/10.1016/j.cose.2018.10.005

Nemati, H. R., Steiger, D. M., Iyer, L. S., & Herschel, R. T. (2002, 2002/06/01/). Knowledge warehouse: an architectural integration of knowledge management, decision support, artificial intelligence and data warehousing. *Decision Support Systems, 33*(2), 143-161. https://doi.org/https://doi.org/10.1016/S0167-9236(01)00141-5

NIST Joint Task Force. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

NIST Joint Task Force. (2020). *Security and Privacy Controls for Information Systems and Organizations*. NIST Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Nunamaker Jr, J. F., Chen, M., & Purdin, T. D. M. (1990, Winter90/91). Systems Development in Information Systems Research [Article]. *Journal of Management Information Systems, 7*(3), 89-106. https://doi.org/10.1080/07421222.1990.11517898

Olphert, W., & Damodaran, L. (2007). Citizen Participation and engagement in the Design of e-Government Services: The Missing Link in Effective ICT Design and Delivery [Article]. *Journal of the Association for Information Systems, 8*(9), 491-507. http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=27677957&site=ehost-live&scope=site

Oostveen, A.-M., & Besselaar, P. v. d. (2004). *From small scale to large scale user participation: a case study of participatory design in e-government systems* Proceedings of the eighth conference on Participatory design: Artful integration: interweaving media, materials and practices - Volume 1, Toronto, Ontario, Canada.

Orozco, D. (2016, Spring2016). The Use of Legal Crowdsourcing ('Lawsourcing') to Achieve Legal, Regulatory, and Policy Objectives [Article]. *American Business Law Journal, 53*(1), 145-192. https://doi.org/10.1111/ablj.12074

Panda, P., & Sahu, G. P. (2013). Critical Success Factors for e-Gov Project: A Unified Model [Article]. *IUP Journal of Supply Chain Management, 10*(2), 19-32. http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=89521613&site=ehost-live&scope=site

Papp, G., El-Gayar, O., & Lovaas, P. (2020). *Citizen Trust in the United States Government: Twitter Analytics Measuring Trust in Government Sentiments* AMCIS 2020 Proceedings, https://aisel.aisnet.org/amcis2020/social_computing/social_computing/13

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45. https://doi.org/10.2753/MIS0742-1222240302

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design Science Research Evaluation. Design Science Research in Information Systems. Advances in Theory and Practice, Berlin, Heidelberg.

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020, November 2020). *Workforce Framework for Cybersecurity (NICE Framework)*. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Polletta, F., & Gardner, B. (2018). The Forms of Deliberative Communication. *The Oxford Handbook of Deliberative Democracy*.

Porwol, L., Ojo, A., & Breslin, J. (2013). *Harnessing the duality of e-participation: social software infrastructure design* Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance, Seoul, Republic of Korea.

Prasad, K. (2012). E-Governance Policy for Modernizing Government through Digital Democracy in India. *Journal of Information Policy, 2*, 183-203. https://doi.org/10.5325/jinfopoli.2.2012.0183

Prier, J. (2017). Commanding the Trend Social Media as Information Warfare. *Strategic Studies Quarterly, 11*(4), 50-85. http://www.jstor.org.ezproxy.niagara.edu/stable/26271634

Putnam, R. D. (2001). *Bowling Alone: Revised and Updated : The Collapse and Revival of American Community*. Simon & Schuster. http://ebookcentral.proquest.com/lib/niagara-ebooks/detail.action?docID=4935299

Robertson, S. P. (2005). Voter-centered design: Toward a voter decision support system. *ACM Trans. Comput.-Hum. Interact., 12*(2), 263-292. https://doi.org/10.1145/1067860.1067866

Salvino, R., Tasto, M. T., & Turnbull, G. K. (2012, 2012/06/01). A direct test of direct democracy: New England town meetings. *Applied Economics, 44*(18), 2393-2402. https://doi.org/10.1080/00036846.2011.564148

Shim, J. P., Warkentin, M., Courtney, J. F., Power, D. J., Sharda, R., & Carlsson, C. (2002, 2002/06/01/). Past, present, and future of decision support technology. *Decision Support Systems, 33*(2), 111-126. https://doi.org/https://doi.org/10.1016/S0167-9236(01)00139-7

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly, 35*(4), 989-1015. https://doi.org/10.2307/41409970

Sprague, R. H., & Carlson, E. D. (1982). Building Effective Decision Support Systems.

Starke, C., Marcinkowski, F., & Wintterlin, F. (2020, Apr 2020, 2021-03-09). Social Networking Sites, Personalization, and Trust in Government: Empirical Evidence for a Mediation Model. *Social Media + Society, 6*(2). https://doi.org/http://dx.doi.org/10.1177/2056305120913885

Sudhipongpracha, T. (2018, 2018/09/02). Exploring the effects of coproduction on citizen trust in government a cross-national comparison of community-based diabetes prevention programmes in Thailand and the United States. *Journal of Asian Public Policy, 11*(3), 350-368. https://doi.org/10.1080/17516234.2018.1429237

Supriyanto, A., Diartono, D. A., Hartono, B., & Februariyanti, H. (2019, 29-30 Oct. 2019). Inclusive Security Models To Building E-Government Trust. 2019 3rd International Conference on Informatics and Computational Sciences (ICICoS),

Tassabehji, R., Elliman, T., & Mellor, J. (2007). Generating Citizen Trust in E-Government Security: Challenging Perceptions. *International Journal of Cases on Electronic Commerce, 3*(3), 1-17.

Teo, T. S. H., Srivastava, S. C., & Jiang, L. I. (2008, Winter2008). Trust and Electronic Government Success: An Empirical Study [Article]. *Journal of Management Information Systems, 25*(3), 99-131. https://doi.org/10.2753/MIS0742-1222250303

Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S., & Serna, J. (2018). *PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation* Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, Tempe, AZ, USA.

The White House. (2023, March). National Cybersecurity Strategy. Retrieved March 11, 2023, from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Thomas, C. W. (1998, May 1998, 2016-06-25). Maintaining and restoring public trust in government agencies and their employees. *Administration & Society, 30*(2), 166-193. https://ezproxy.niagara.edu/login?url=https://search.proquest.com/docview/196838681?accountid=28213

Tolbert, C. J., & Mossberger, K. (2006). The Effects of E-Government on Trust and Confidence in Government [Article]. *Public Administration Review, 66*(3), 354-369. https://doi.org/10.1111/j.1540-6210.2006.00594.x

US Department of Homeland Security (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. DHS NCCIC/ICS-CERT Retrieved from https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

US National Security Agency (2015). *Defense in Depth*. U.S. National Security Agency Retrieved from https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm

Vaishnavi, V. (2008). *Design science research methods and patterns : innovating information and communication technology*. Boca Raton : Auerbach Publications.

Zheng, Y., Schachter, H. L., & Holzer, M. (2014, 2014/10/01/). The impact of government form on e-participation: A study of New Jersey municipalities. *Government Information Quarterly, 31*(4), 653-659. https://doi.org/https://doi.org/10.1016/j.giq.2014.06.004