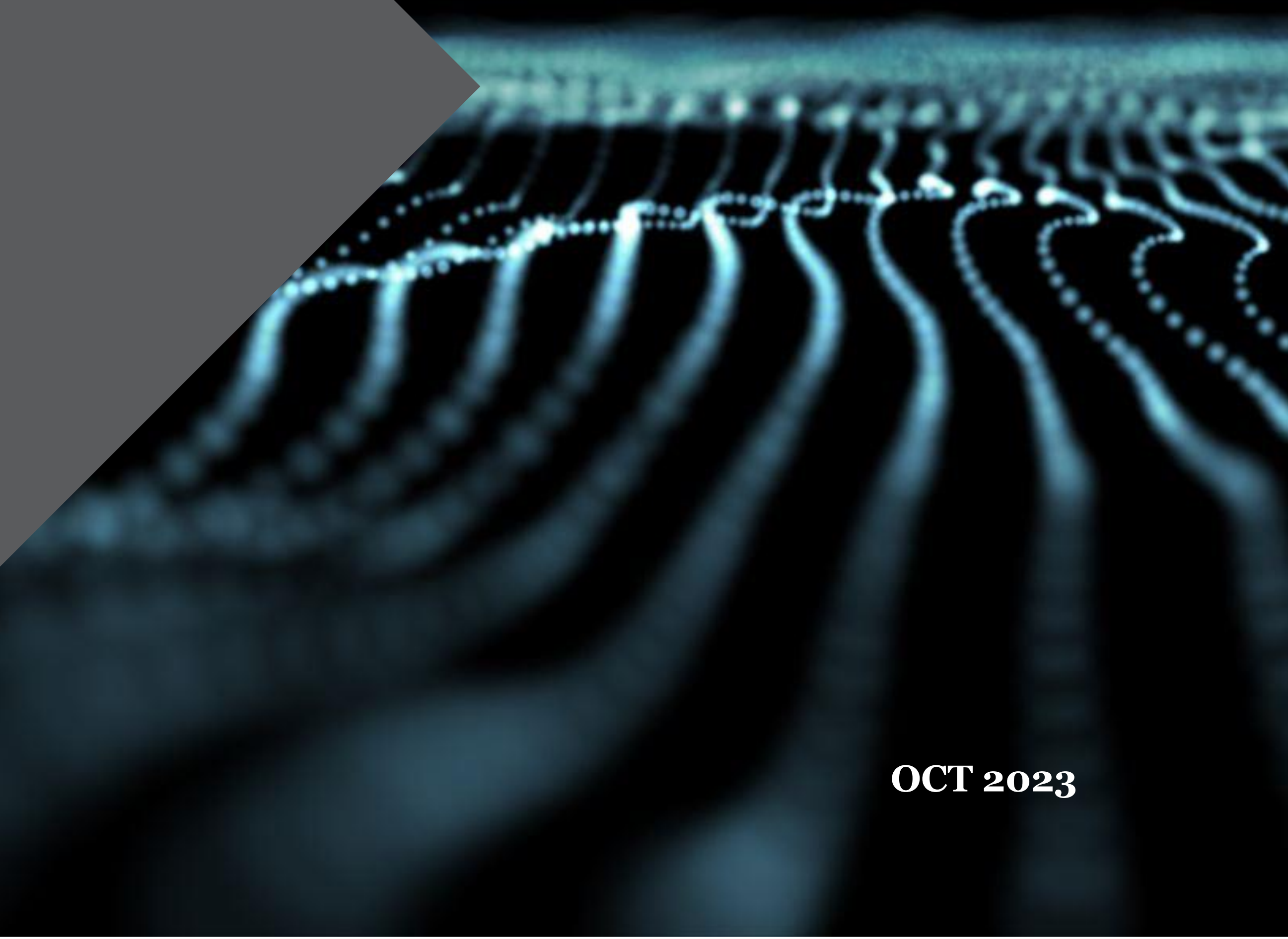
Homeland Security

HOW TO WRITE A CONNECTED COMMUNITY STRATEGY

Ver 1.0



OCT 2023

TABLE OF CONTENTS

PART ONE: SETTING THE FOUNDATION FOR THE CONNECTED COMMUNITY

PART TWO: CHARTING A ROADMAP TO SUCCESS

PART THREE: DO NO HARM

HOW TO WRITE A CONNECTED COMMUNITY STRATEGY

Contributions By:

Albert Gehami, City Privacy Officer, City of San Jose, CA

Augustine Boateng, Deputy Chief Information Officer, City of Memphis, TN

Jim Ingraham, Vice President of Strategic Research, EPB, Chattanooga, TN

Kevin Comstock, Director of Transportation Systems, KCI Technologies, Chattanooga, TN

Wendy Harris, Chief Information Officer, City of Memphis, TN

William Plank, Community Economist, EPB, Chattanooga, TN

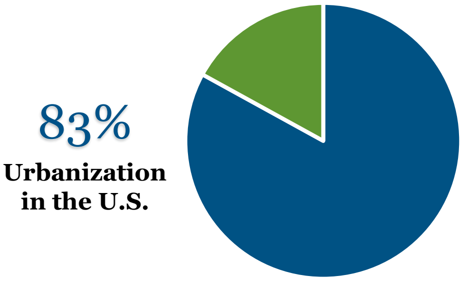
Colorado State University, Fort Collins, CO

NYC Office of Technology Innovation, City of New York, NY

Homeland Security

INTRODUCTION

More than eight billion people live on Earth, and more than half live in metropolitan areas. Currently, 83% of US residents live in some type of urban environment – that number is expected to grow to 89% by 2050[i]. As urbanization accelerates, the demand for infrastructure will also increase. In response, community planners are rapidly turning to digital technology to meet the growing demands of urban life.



Enter the “connected community” – the promise that equitable, safe, secure, and sustainable community life can be achieved through digitization. However, a digital transformation from a traditional community to a connected community requires a robust strategy. Digital strategies help community planners reflect on the factors that must be addressed to foster a connected community. Furthermore, strategies can catalyze the widespread adoption of technical solutions to enhance the community.

A strategy can also be the difference between secure community services and the disruption of those services by cybercriminals. The deployment of new technologies in communities creates new targets of opportunity for cybercriminals. In fact, U.S. state and local governments reported a 70% increase in ransomware attacks between 2020 and 2021. While a digital strategy may not have prevented each attack, a strategy would better prepare community planners to think through the implications of digital projects, which include cyber risks.

Unfortunately, a Department of Homeland Security (DHS) 2023 analysis of 106 of the largest U.S. communities found that only 26 had published a digital transformation strategy as of April 2023. However, all analyzed communities had launched at least one connected community project, suggesting that many projects are started without a comprehensive digital strategy. The analysis does not suggest those projects will fail or lead to cyber-attacks. However, DHS believes that more can be done to foster safe and secure connected communities – and that starts with a strategy.

To that end, DHS partnered with representatives from New York (NY), San Jose (CA), Memphis (TN), Chattanooga (TN), and Colorado State University to develop this "how-to" guide to help community leaders build a digital transformation strategy. Contributors include chief information officers, chief information security officers, chief privacy officers, economists, technology experts, cyber policy professionals, risk analysts, and former municipal executives, each with unique experience driving community digital transformations. This foundational guide is the first in a series of guides that DHS hopes will help communities achieve their connected community goals.

The Audience for this Guide

The primary audience for this guide is municipal leaders and professionals accountable for providing community services. This guide applies to all communities, including suburban localities, small-medium sized cities, mega-cities, and all communities in between. Finally, this is not a prescriptive guide; instead, the guide provides best-practice advice from experts nationwide to help community planners navigate a municipal digital transformation. Should you have questions about this document, please contact the DHS Emerging Technology Policy Team at et_plcy@hq.dhs.gov

The Audience for a Connected Community Strategy

While the audience for this "how-to" guide is community planners, the audience for a connected community strategy based on this guide should always be community residents and community stakeholders. Therefore, a successful connected community strategy should provide the readers with the "who, what, when, where, and why" of a connected community transformation.

A Note on "Connected Communities"

Connected communities are communities of all sizes that leverage digital technology and data to address community needs. For the purposes of this guide, we use the term "Connected communities," as it is more inclusive than "smart cities." The term "smart city" often emphasizes large metropolitan areas at the exclusion of small towns and rural communities. References to "connected communities" in this guide include mega-cities, rural communities, and all other places where U.S. residents make their homes.

PART ONE: SETTING THE FOUNDATION FOR THE CONNECTED COMMUNITY

An effective connected community strategy starts with a strong foundation. The foundation of a connected community strategy consists of three items: an articulated vision, defined community values, and a clear description of the community's current characteristics. When taken together, these three concepts will inform the overall strategy for a community's digital transformation.

Articulate a Connected Community Vision

A “vision” describes the desired future state for a community. A connected community vision should be clear, understandable, inspirational, motivational, and forward-looking. Furthermore, a good vision should clearly articulate the incentives and benefits residents should expect from living in a connected community. Additionally, a connected community vision should be relevant and unique to the community seeking a digital transformation.

> *“IN OUR THIRD CENTURY, MEMPHIS WILL BUILD UP, NOT OUT. Memphis will be a city that anchors growth on strengths of the core and neighborhoods; a city of greater connectivity and access; a city of opportunity for all.”*
>
> *Vision Statement   Memphis3.0 Comprehensive Plan*

Define the Community’s Values

Community values are the principles, norms, and mores that guide actions within a community. A connected community vision and values will provide a unified framework that guides the connected community strategy. A connected community strategy should clearly articulate values so residents understand what is important (i.e., a code of conduct). Community planners might consider the following values when developing a connected community strategy:

- **Equality & Equity:** Connected communities distribute resources to foster equality of opportunity.
- **Accessibility:** Connected community services are intuitive, user-centric, and inclusive of differently abled and underserved groups.
- **Transparency:** Connected community leaders are open, honest, and authentic in articulating projects and programs.
- **Sustainability & Efficiency:** Digital services are maintainable over time while mitigating the environmental impacts of community life.
- **Protection from Harm:** Community leaders protect civil rights and mitigate the potential risks of community digitization.
- **Accountability:** Community leaders are held to standards of excellence and ethics when providing community services.
- **Community Participation:** Community residents have a voice in transforming their community into a connected community.

The above values are only examples. Like a connected community vision, connected community values should be unique and relevant to each community. The City of Memphis' "Memphis3.0 Comprehensive Plan" provides an illustrative example of values that are unique to Memphis.

> ***"Memphis is a city that VALUES LAND AS AN ASSET.***
> *Memphis cannot continue its growth policy of the past. The City will succeed by creating compact communities where land use and density support walkable, active, and transit served communities."*

> ***"Memphis is a city of CONNECTED COMMUNITIES.***
> *Memphis communities desire greater connectivity and access. For Memphis to thrive, it must expand residents' ability to connect to mobility options, opportunity, and one another."*

> ***"Memphis is a city of EQUITY AND OPPORTUNITY.***
> *Through actions, investments, and citizen-led neighborhood interventions, historically disadvantaged communities must gain greater access to resources and opportunities to succeed and prosper."*

Describe the Community's Current Situation

A clear vision and values provide community residents with the answer to the question, "where do we want to be?" However, planners must first understand "where we are" today to build a connected community strategy. Answering that question requires a diligent assessment of the characteristics of the community. A clear articulation of the shape and features of the community allows planners to identify areas that could benefit from digitization.

Planners should consider the following variables when assessing their community's current situation and characteristics:

- Municipal services and utilities such as public safety, water, and sanitation.
- Physical infrastructure such as buildings and service-supporting infrastructure.

- Digital infrastructure like IT assets and telecommunications networks.
- Jurisdictions with authority over services, infrastructure, and land.
- Stakeholders, especially the community residents.
- Demographics and population distributions.
- Existing budgets and funding.
- Community leadership priorities.
- Available datasets.

Planners can start their analyses by focusing on their community's municipal services and the critical systems underpinning those services. For example, New York City's (NYC) 911 system is the nation's most extensive emergency communication system and serves approximately nine million calls annually. The advent of mobile devices has made managing NYC's traditional 911 call system more complex. As a result, NYC has elected to implement a Next-Generation 911 (NG911) call system to accommodate digital and mobile communications.[ii]

Planners can also begin their analyses based on existing community priorities. For example, the current budget cycle or the election of a new mayoral administration will likely inform a connected community analysis.

Finally, planners should consider adopting a "consumer-centric" approach to their analyses. Departmental missions and administrative priorities are all factors to consider when planning a connected community transformation. However, planners should always remember that communities provide services to improve the lives of real people. Therefore, planners could assess how municipal resources are consumed or focus analyses on traditionally underserved communities.

Regardless of how planners frame their analyses – they will still need data and information. Data and information come in multiple forms and from multiple data sources, and planners should prepare to leverage all data sources at their disposal. For example:

- **Data from Community Service Providers:** The departments and agencies that provide services to communities will store data that will benefit analyses. For example, departments responsible for housing might have data related to demographics, underserved communities, and quality of life metrics.
- **Primary Sources of Data:** Data obtained directly from community residents provides more significant insights into their needs and promotes greater community participation. Planners should consider conducting on-the-ground surveys to provide context and more nuance to data that municipal service providers might collect. Town Halls or focus groups are also excellent methods of gathering direct data from community residents.
- **Federal Government Sources:** The federal government is also an excellent data source to inform analyses. For example, the Federal Open Government program (Data.gov) provides access to over 200,000 datasets, including Census

data and data related to nationwide broadband access, climate impacts, and economic justice.

Planners should make special considerations when collecting and using data in their assessments. The data discovery process should begin as early as possible, and planners should strive to streamline information sharing across stakeholders. Planners should also recognize that some data, such as census data, will be more "static." In contrast, other data points will be dynamic and serve only as a snapshot in time. Additionally, planners should carefully consider the data sources as the source may provide helpful context or introduce biases. Finally, planners should remember that a finished connected community strategy will be a public document – Therefore, planners should strive to balance transparency with data confidentiality.

Assessing the unique characteristics of your community is a challenging feat. However, the importance of this assessment cannot be overstated. A clear understanding of the community can be the difference between a successful digital transformation and costly project failures. However, when planners complete a community assessment, they will have a clearer understanding of the gaps between where the community is now and the connected community vision. The identified gaps then become the roadmap for your connected community strategy.

Part One Conclusion

Part one of this guide introduces the concept of connected communities and describes how planners can set the foundation for a strong strategy. The first three steps of building a connected community strategy are as follows: (1) articulate a connected community vision; (2) define the community's values; and (3) describe the community's current state. When taken together, these three steps will help planners build a roadmap for a connected community transformation.

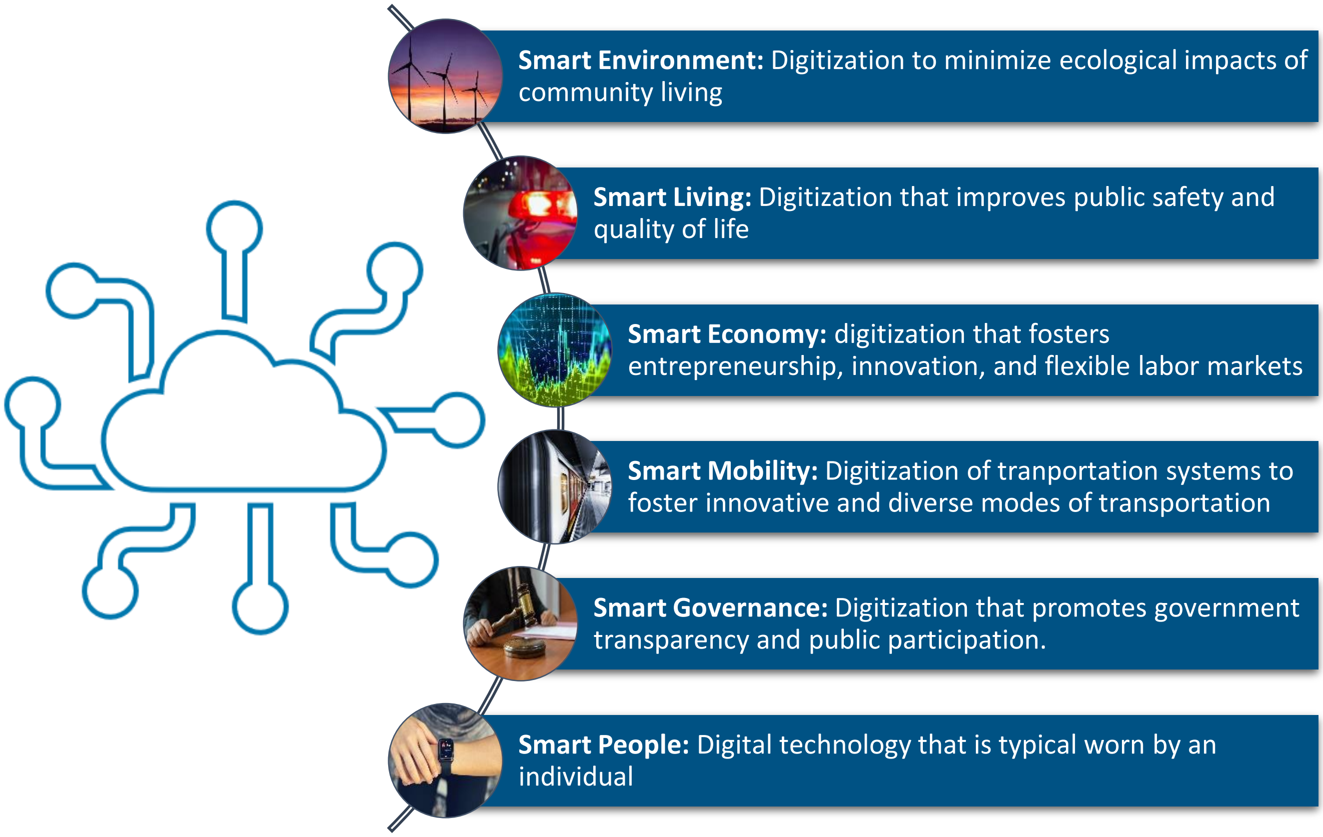
PART TWO: CHARTING A ROADMAP TO SUCCESS

Vision statements, values, and community assessments are only helpful insofar as the information informs an actual plan. Planners ultimately need to take the analysis from part one and build a roadmap for progress toward the connected community vision. There are four actions that planners should take to build a roadmap: define smart service areas, articulate objectives & metrics, engage stakeholders, and outline a communications plan.

Define “Smart” Service Areas

Connected communities use data and information communications technology to enhance community services. Colloquially, these digitally enhanced services are called “smart services.” Digital technology offers planners a wide variety of tools to solve community challenges. As such, the variety of "smart services" a community might offer is limited only by a planner’s creativity and the available technology. That same variety can also complicate the process of planning and managing projects. For example, a community might choose to deploy smart streetlights that dynamically change the brightness of bulbs, host public Wi-Fi, and integrate an emergency notification system. The variable capabilities of a smart streetlight might make it difficult to determine who is responsible for funding, implementing, and maintaining that project.

To address this complexity, planners should define service areas to categorize proposed projects. Once smart service areas are clearly defined, projects can be aligned based on service areas and the desired outcome of a given project. There are several existing frameworks for defining “smart” services – one such taxonomy is provided below:



Smart Environment: Digitization to minimize ecological impacts of community living

Smart Living: Digitization that improves public safety and quality of life

Smart Economy: digitization that fosters entrepreneurship, innovation, and flexible labor markets

Smart Mobility: Digitization of tranportation systems to foster innovative and diverse modes of transportation

Smart Governance: Digitization that promotes government transparency and public participation.

Smart People: Digital technology that is typical worn by an individual

For example, "Smart Mobility" as a service area uses digital technology to provide diverse forms of public transportation for community residents. “Smart Mobility” might include autonomous trams encountered at airports, ride-sharing applications, E-bike sharing programs, and many other digital innovations that enhance transportation services. NYC provides an illustrative example of a “Smart Mobility” project – specifically NYC’s Transit Signal Priority (TSP) program. NYC has improved the daily bus commute for millions of New Yorkers by equipping city buses and traffic lights with real-time sensors that prioritize bus transit through signalized intersections.[iii]

The above taxonomy is only an example; planners should define service areas in a way that makes sense for their communities and drives the implementation of their strategy. Planners should also remember some smart projects impact multiple utilities and will, therefore, fall within multiple smart service areas. For example, NYC TSP is a smart mobility project. However, TSP might increase mass transit use, positively impacting the environment. As such, the TSP could also be considered a "Smart Environment" project. Ultimately, planners should ensure that whatever breakdown they choose is intuitive enough to be understood by the strategy's primary audience – the community residents.

Defining smart services offers several benefits to the planner when developing a connected community strategy. First, defined smart service areas can help orient and create a shared vision for the community employees responsible for projects. Smart service areas can also serve as a framework for planners to assess the current and desired end state of existing community functions. Defining service areas can also inform who should fund a smart project and who should maintain the implemented service over time. Finally, defined smart service areas allow planners to communicate the purpose of individual smart projects more easily to community stakeholders.

Articulate Objectives and Metrics

A strategy without measures of success is no strategy at all. Therefore, a strong connected community strategy must also include a plan for measuring progress toward an articulated vision. Measuring progress, first and foremost, requires a clear identification and articulation of discreet objectives. Objectives drive strategy implementation and resource allocation. Furthermore, objectives allow community planners to communicate to stakeholders how every smart project adds value.

Objectives also inform metrics used to measure progress toward connected community goals. Metrics will help planners understand where the community has been and where the community is going. Additionally, metrics will help highlight when plans are going well and when those plans are not achieving desired outcomes.

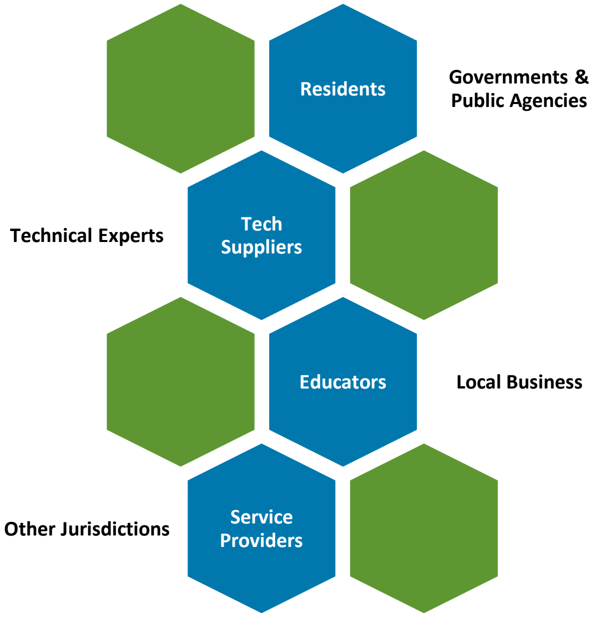
The range of metrics a community might track can vary drastically. A community can base metrics on mandatory requirements such as those articulated by law or local appropriation processes. Communities can develop metrics based on the delivery of community services. Communities can develop metrics based on the delivery of services to track how effectively the community adopts new technology. Ultimately, there is no single "correct" set of metrics for a connected community to track. Overall, metrics should be consistent with defined objectives and support the implementation of the connected community strategy.

Several approaches to developing objectives and metrics to track connected community goals exist. For example, The National Institute of Standards and Technology (NIST) Special Publication 1900-206, "Smart Cities and Communities: A Key Performance Indicators Framework," introduces a framework by which communities can assess the benefits of "smart" technologies. The NIST framework builds on conventional key performance indicator methods while accounting for factors that vary across communities, such as variable neighborhood sizes, population densities, and economies.[iv]

Objectives and metrics are critical to an effective connected community strategy; however, planners should not measure simply for the sake of measuring. For example, community planners may want to reduce pedestrian accidents and choose to deploy smart traffic lights to achieve that objective. Tracking the number of smart traffic lights deployed in a neighborhood is important; however, that metric lacks meaning without context. The important metric is the overall reduction or lack thereof in pedestrian accidents. Ultimately, the objectives and metrics are about driving positive outcomes for a connected community.

Identify and Plan to Engage with Stakeholders

Multiple groups will impact and be impacted by any connected community project. These groups are typically called stakeholders and will be interested in the outcome of connected community transformation. Stakeholders will vary from community to community; however, stakeholders generally include:



The HCS (Hamilton County Schools) EdConnect program provides an illustrative example of stakeholder engagement to address the digital divide. A partnership between EPB of Chattanooga, the City of Chattanooga, and Hamilton County, Tennessee, HCS EdConnect was launched in 2020 amid the COVID-19 pandemic to ensure access to high-speed internet at no cost for qualifying K-12 students in need on EPB's community-wide fiber-to-the-home network. Today, HCS EdConnect serves 28,000 people, including children and their family members, and continues as a permanent program with wide-ranging support from private and public entities. In addition to helping children keep up with assignments, parents utilize HCS EConnect to support their students through stronger parent-teacher engagement, according to preliminary surveys conducted by the University of Tennessee at Chattanooga and Boston College. These surveys also found that households participating in the EdConnect program benefit from access to health resources and job opportunities found online. In short, EPB of Chattanooga engaged multiple stakeholders to provide a critical digital service to city residents through free broadband for students.[v]

The importance of stakeholder engagement cannot be overstated, and the HCS EdConnect program is an example of the benefits of engagement. The number and influence of stakeholders will vary between communities. Accounting for and addressing these stakeholders' equities can determine a smart project's success. Therefore, planners should identify and engage with stakeholders early and often.

Outline a Communications Plan

Core to stakeholder engagement is communication, and a strong connected community strategy should always include a robust communications plan. Communication plans serve several purposes – among the most important is transparency. A connected community strategy will impact resident's lives. Connected community technology typically uses data, and that data is most often generated by residents going about their daily lives. Therefore, planners must allow community residents to make informed decisions about their interactions with community technology whenever possible. Residents can only make informed decisions when kept informed – and this can only be achieved through a well-thought-out communications plan.

In addition to transparency, a good communication plan should include an educational component. Education is part and parcel of encouraging residents to be informed participants in a community's digital transformation. For example, how residents use a new digital service may not be apparent and understandable to those residents. In these situations, digital literacy becomes an important factor in ensuring the success of a project. Fostering digital literacy through education should be part of a robust communications plan.

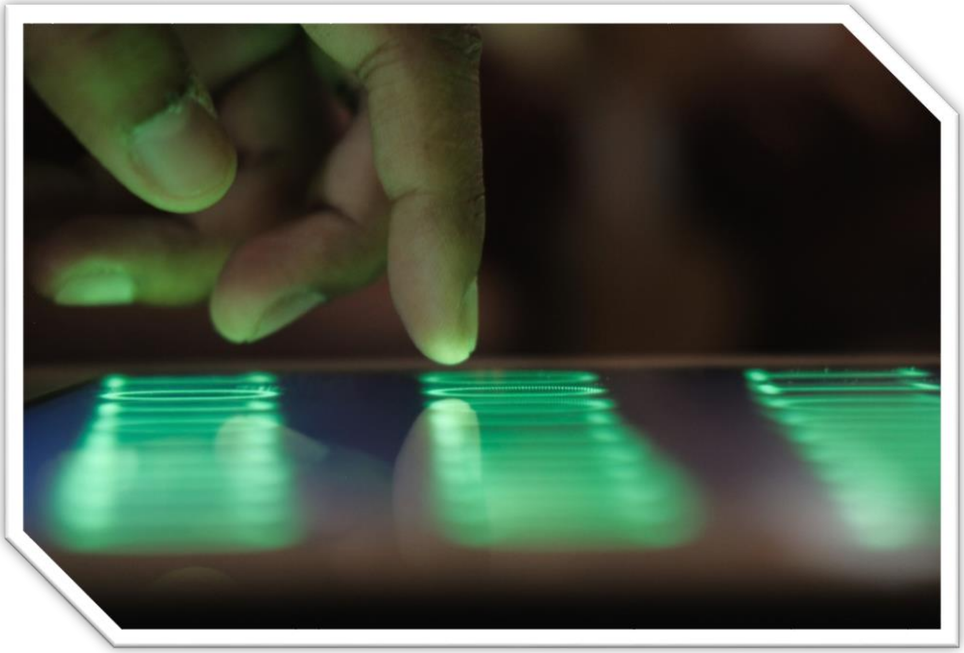
Part Two Conclusion

The roadmap is arguably the most important component of the connected community strategy. Vision and values are important; however, these ideas are merely aspirations without a plan. The roadmap is ultimately the plan for how communities will achieve their aspirations. Planners should consider four elements when building a connected community strategy roadmap: (1) define smart service areas; (2) articulate objectives and metrics; (3) engage stakeholders; and (4) outline a communication plan.

PART THREE: DO NO HARM

This guide heretofore has discussed how to position a community to modernize and take advantage of digital technology. However, the advantages of digital technologies also come with digital risks. The vast amounts of consumer data and the criticality of services have made communities ideal targets for cybercriminals. According to the Verizon 2021 Data Breach Investigations Report (DBIR),[vi] at least 2323 local governments, public schools, and healthcare providers were disrupted by ransomware attacks in 2021. It is estimated that the average cost of a security breach to a State is between $665,000 and $40.53 million[vii] – that is to say, nothing of the very real yet non-financial impact on the lives of residents.

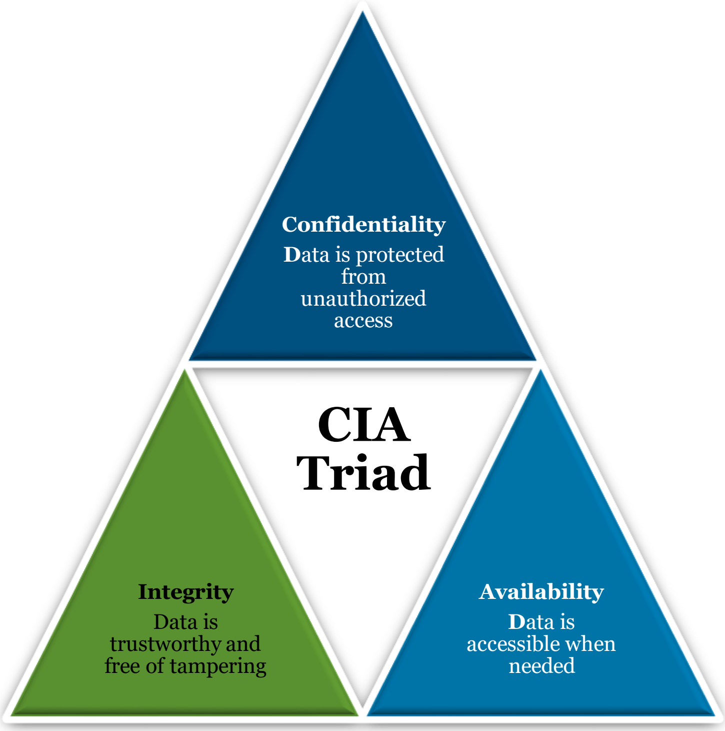
The local governments that manage communities are ideal targets for cybercriminals. However, poorly managed governments can also present a potential risk to community residents. Local governments, amongst other critical services, are responsible for law enforcement, housing, education, and emergency management services. These services can positively or negatively impact lives depending on how governments execute their authority. Digitization of services will only increase the potential impact governments can have on residents' lives. Therefore, it is incumbent upon those in power to acknowledge the harms that digitization can introduce and include mitigation plans in a connected community strategy.



Plan for Secure-by-Design Smart Services

A connected community transformation can provide significant benefits to residents, but transformation can also introduce digital risks. For example, an internet-enabled NG911 system can accommodate text, images, and video, which improves services over traditional 911 call centers. However, NG911 call centers are also susceptible to cyber-attacks. Researchers at Ben-Gurion University of the Negev found that a distributed denial of service (DDoS) attack launched by only 6,000 bots could disrupt a NG911 system.[viii] This is a risk that does not exist in traditional 911 systems. Essentially, a community adopting NG911 systems can introduce cyber risks to emergency services where no such risk existed previously.

Community planners and governing bodies have a responsibility not to expose residents to unnecessary risks. Therefore, planners should strive for connected community projects that are secure-by-design and secure-by-default. Planners should adopt technology with security as a core feature and implement that technology so that security is at the forefront of digital services. The breadth and variety of "smart" technology that can be deployed in a connected community are vast; as a result, this guide cannot provide specifics for securing every possible connected community technology. However, some high-level security principles apply to digital technology regardless of the use case. One set of principles that planners should consider is the "CIA Cybersecurity Triad." The CIA Triad, which stands for confidentiality, integrity, and availability, is a model for guiding cybersecurity functions for an organization.


Confidentiality
Data is protected from unauthorized access
CIA Triad
Integrity
Data is trustworthy and free of tampering
Availability
Data is accessible when needed

There is more to the CIA Triad than the definitions provided. “Confidentiality,” at its core, is about restricting access to data to only those authorized to have access. In layperson's terms, a loss of confidentiality means data has been seen by someone not authorized to see the data. In the world of information security, confidentiality is achieved through authentication and authorization.

Authentication is the process by which a system determines a user is who they claim to be. Authentication requirements are a part of everyday modern life. Every email login and mobile phone passcode are examples of authentication requirements. Several methods exist to authenticate users, including passwords, biometrics such as fingerprint scanners, tokens such as smart cards, and a panoply of cryptographic techniques. The authentication method will ultimately depend on the system in question and the level of data protection required.

Authorization, conversely, determines if the user has the right to access data. A user can be successfully authenticated and still not have authorization to use a system or data. Authorization will require planners to identify who needs access to data generated by a community and set restrictions accordingly. Fortunately, many of the same techniques that authenticate a user can be used to determine that user’s authorization for data access.

“Integrity” techniques ensure that data is accurate and in the correct format. Many of the same techniques used to ensure the “confidentiality” of data will also enforce data integrity. For example, a user who cannot access data will be unable to manipulate that data. A key technique for ensuring data integrity is regular data backups that allow system owners to revert to a known “good state” when unauthorized changes to data are detected.

Finally, “availability” techniques ensure authorized users and systems have access to data when the data is needed. Traditionally, availability techniques fell within the remit of non-security information technology professionals. For example, managing network bandwidth and providing failover capacity is typically done by a community’s IT professionals. However, non-ethical cyber actors can compromise data availability, such as using DDoS attacks outlined at the start of this section. Furthermore, data availability takes on increased importance when that data is used to provide critical community services such as 911 and other emergency management services. Therefore, planners should place as much emphasis on data availability as they do on data confidentiality and integrity.

The CIA Triad can be a framework to help planners reflect on the potential cybersecurity risks and risk mitigations for a proposed project. For every "smart" project, planners should articulate plans to protect the confidentiality, integrity, and availability of the underlying data that make those projects a reality. These considerations should apply across the full scope of technology that supports a connected community, including:

SENSORS & IOT

EDGE DEVICES

DATA CENTERS

OPERATIONAL TECHNOLOGY

CLOUD SYSTEMS

COMMAND CENTERS

COMMUNICATIONS INFRASTRUCTURE

Furthermore, connected community planners should consider various security and resilience techniques that support multiple CIA Triad principles. For example, endpoint protection tools like antivirus software can mitigate the risks of malware that could compromise the confidentiality, availability, and integrity of data. Incident response and disaster recovery plans are also important components of ensuring connected community services are available when residents need those services.

The importance of security in connected communities cannot be overstated. For example, the ransomware group Play allegedly launched an attack on a large US municipality in 2023, resulting in the loss of data confidentiality, integrity, and availability. The ransomware attack encrypted the municipality's data (loss of integrity), disrupting multiple municipal services (loss of availability). To make matters worse, the ransomware group also stole municipal data, which included personally identifiable information about municipal employees and residents. Play then released the data on the dark web (loss of confidentiality).

Play's actions were not a one-off event. According to data collected by cybersecurity firm SecurLore, 44 states and 227 local governments were victimized by malicious cyber actors between September 2021 and September 2023.[ix] Cyber-attacks on communities will likely increase in frequency as more communities adopt digital technologies. Therefore, it is paramount that connected community planners consider security and safety up-front when planning digital transformations.

Give Special Consideration to Privacy Concerns

As discussed, governments that manage communities hold unique authority compared to private industry. In various circumstances, governments can lawfully deprive residents of their freedoms, property, liberties, and lives. Therefore, governments are responsible for considering data ethics - specifically data privacy. Data privacy technically falls under the umbrella of "confidentiality" in the CIA triad; however, the vast quantities of data collected in a connected community elevates the importance of digital privacy. As such, planners should develop and articulate privacy principles as part of the connected community strategy. Generally, privacy principles should strive to:

- Minimize the amount of data collected.
- Minimize how long data is held.
- Foster transparency in data collection and use.
- Limit data use to only stated purposes and per community values.
- Promote accuracy and completeness in data.
- Maintain the security of data.

Privacy principles are an important first step; however, a plan is required to implement those principles. For example, The City of San Jose's Digital Privacy Policy consists of seven elements: notice of collection, defined retention periods, collection minimization, data accountability, accuracy in use, responsible data sharing, and advancing equity through data-driven decisions.[x] However, San Jose did not only publish privacy principles; The city put those principles into practice through policy and comprehensive digital privacy manuals.

The decisions that governments at all levels make impact residents, and residents have a fundamental right to privacy. Thus, community planners have a critical responsibility to protect residents' privacy. Planners must inform residents how data will be collected, used, and retained. Additionally, residents must be allowed to make informed decisions about their data. Ultimately, privacy principles are about safeguarding public trust in community services and protecting digital privacy.

Identify Accountable Officers

Strategies are only meaningful if someone is held accountable and empowered to act. Accountability is especially important when mitigating risks associated with a connected community transformation. Planners should consider three roles to properly address the potential harms that a connected community strategy might introduce:

- The Chief Technology Officer: the executive who determines and is accountable for a community's technology strategy.
- The Chief Information Security Officer: the executive responsible for driving cybersecurity strategies and the security of a community's digital assets.
- The Chief Privacy Officer: the executive responsible for policies and programs that protect the privacy of residents and community employees.

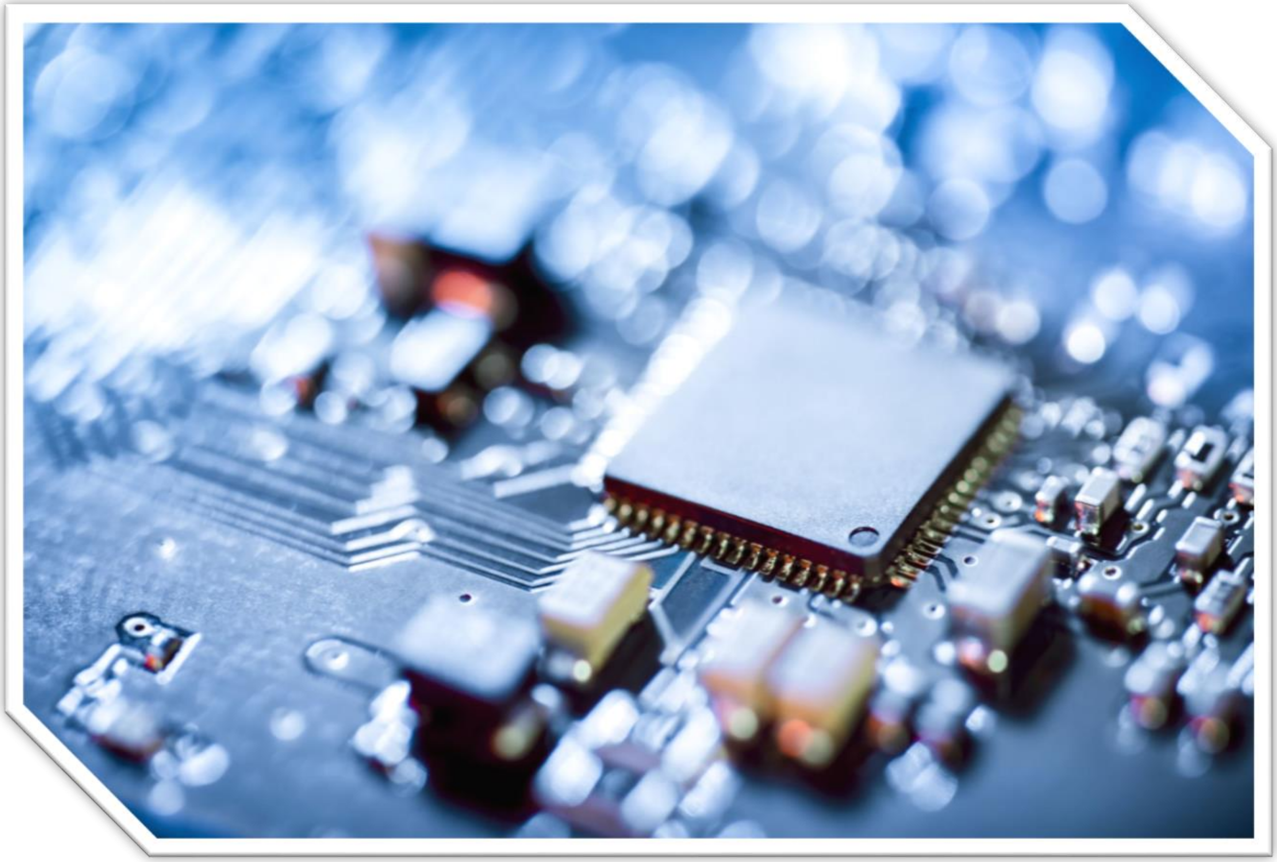
Each role's exact function and make-up will vary from community to community. For example, the City of New York's Office of Privacy and NYC Cyber Command are led by the city's Chief Privacy Officer and Chief Information Security Officer, respectively. These leaders report to the city's Chief Technology Officer, who coordinates technology-related projects and policies. A community smaller than NYC might be unable to support fully staffed offices dedicated to technology, privacy, and cybersecurity. However, accountability structures can be different across communities. All that is important is that planners consider who is responsible for what activity, clearly articulate that responsibility in the overall strategy, and plan to empower individuals accordingly.

Part Three Conclusion

Connected communities and the digital technologies that support those communities have the potential to enhance the lives of residents. However, the harms that the widespread use of digital technology might introduce can undercut the benefits provided by a connected community. Planners ultimately must take steps to mitigate the potential harms of digital technology as part of the larger connected community strategy. Planners should consider three elements when building harm reduction into the connected community strategy: (1) plan for projects to be secure-by-design; (2) give special attention to digital privacy; and (3) identify accountable officers for cybersecurity and privacy.

FINAL THOUGHTS

Digital technologies and the connected community movement can potentially improve the lives of residents across the U.S. However, the benefits promised by connected communities can only be achieved through planning and actionable strategies. The myriad of connected community considerations can seem overwhelming, yet a few foundational principles can help planners start the journey toward a connected community. This guide, drafted in collaboration with practitioners from municipalities across the U.S., is an attempt to provide foundational guidance to community planners.



Planners should consider ten elements when developing their connected strategies:

- **Articulate a Connected Community Vision**
- **Define the Community's Values**
- **Describe the Community's Current Situation**
- **Define "Smart" Service Areas**
- **Articulate Objectives and Metrics**
- **Identify and Plan to Engage with Stakeholders**
- **Outline a Communications Plan**
- **Plan for Secure-by-Design Smart Services**
- **Give Special Consideration to Privacy Concerns**
- **Identify Accountable Officers**

These ten elements form the foundation for an effective connected community strategy, and an effective strategy often leads to successful execution. The digitization of our communities is well underway – and that digitization can lead to positive outcomes when properly planned or harms when undertaken ad hoc. DHS and its partners hope that this guide, and future guides, will help communities across the U.S. emerge as safe, sustainable, and secure connected communities of the future.

[i] Center for Sustainable Systems, University of Michigan. 2022. "U.S. Cities Factsheet." Pub. No. CSS09-06

[ii] City of New York. (2022, December 22). NYC's Next Generation 911 on Target for 2024 Completion. NYC Office of Technology and Innovation - Oti. https://www.nyc.gov/content/oti/pages/press-releases/next-gen-911-on-target-2024-completion

[iii] MTA and NYCDOT Announce 2.7 Miles of New Bus Lanes on 149 St and Transit Signal Priority Along the 149 St Corridor. (2020, October 9). MTA; Metropolitan Transportation Authority. https://new.mta.info/mta-and-nycdot-announce-27-miles-new-bus-lanes-149-st-and-transit-signal

[iv] Special Publication (NIST SP) - 1900-206

[v] Chattanooga, E. P. B. (2022, July 19). HCS EdConnect powered by EPB shows positive results for increasing parental engagement in education and more. Epb.com. https://epb.com/newsroom/press-releases/hcs-edconnect-powered-by-epb-shows-positive-results-for-increasing-parental-engagement-in-education-and-more/

[vi] Verizon. (2021). 2021 Data Breach Investigations Report (DBIR). Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

[vii] Eytan, D. O. (2021, June 22). Council Post: Municipal Cyberattacks: A New Threat Or Persistent Risk? Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/06/22/municipal-cyberattacks-a-new-threat-or-persistent-risk/?sh=5b596d843ffb

[viii] Mirsky, Y., & Guri, M. (2020). DDoS Attacks on 9-1-1 Emergency Services. IEEE Transactions on Dependable and Secure Computing, 2767–2786. https://doi.org/10.1109/TDSC.2019.2963856

[ix] Cyber Attack Archive | Resources | SecuLore Solutions. (n.d.). Www.seculore.com. Retrieved September 26, 2023, from https://www.seculore.com/resources/cyber-attack-archive

[x] Digital Privacy | City of San José. (2023, June 22). Www.sanjoseca.gov. https://www.sanjoseca.gov/your-government/departments-offices/information-technology/digital-privacy#:~:text=Maintain%20accountability%20for%20data%20usage