SECURE CLOUD ARCHITECTURE

Towards a Smart City cloud privacy, Security, and Rights-Inclusive Architecture

SC3-cpSRIA ACTION CLUSTER BLUEPRINT v0.7

Smart and Secure City and Community Challenge

Authors/Editors
Lee W McKnight
Syracuse University iSchool
Kevin Bornatsch, WiTec
Authors
Yusuf Saadiq Abdul-Qadir, NYCLU
Sam Edelstein, City of Syracuse
Lan Jenson, Adaptable Security
Action Cluster Contributors
Jeff Choquette, Dell Technologies
Mark Coleman, Syracuse University, Geoff d'Alelio, VMware, Michael DePalma & Richie Etwaru, Hu-manity.co, Phil Evangelista, IBM, Harpreet Geekee, Highmark Global, Darren Orzechowski, IBM Red Hat Angela Rieks and Danielle Smith, Syracuse University, David Shomar, Saab, Vijay Srinivas, Applied Information Security, and colleagues from ANDRO; Central New York Biotech Accelerator CEO (CenterstateCEO) , ColorTokens; Farm to Flame Energy Inc.; FMC Globalsat; iConsult; Imcon International Inc.; Keyed Systems; Kymeta; LifeSource Health; Microsoft; Ngenuity LLC; NineAI; Omnimesh; One Planet Education Network (OPEN); Promptous; State University of New York- College of Environmental Studies and Forestry (SUNY-ESF); SUNY-Oswego; SUNY-Upstate Medical University; WiTec

Publication Date: July 10, 2019

GCTC CPAC SC3-cpSRIA Secure Cloud Architecture Guidelines

Acknowledgements

The GCTC SRIA Secure Cloud Architecture Action Cluster Leadership Team would like to thank the elected officials and the many dedicated public sector employees from the following municipalities and communities for their leadership and support for the initiation of consideration of a Secure Cloud Architecture for smart cities, communities and regions,, and for their support of the work that went into creating this draft blueprint.

- **Mayor Ben Walsh**, City of Syracuse, NY
- **Deputy Mayor Sharon F. Owens** City of Syracuse, NY
- **Carolyn McKnight**, Principal, East Los Angeles Performing Arts Magnet School
  Los Angeles Unified School District

We also offer many thanks to our private-sector, community and university partners, listed above and especially CPAC, the **Cybersecurity and Privacy Advisory Committee (CPAC).** CPAC members include**:** Department of Homeland Security, Adaptable Security Corp, Evo Monitors, EP3 Foundation, Global Cyber Alliance, ISC2 Silicon Valley Chapter, San Mateo County, SF Bay ISSA, Sightlinesec, Smart Connections Consulting, The Sorter Group, SRI International. This Action Cluster would not be possible without the guidance and leadership of CPAC, under whose auspices this Action Cluster offers its work.

The Leadership team would like to recognize the contributions of **Jean Rice** from the National Telecommunications and Information Administration (NTIA) (herself a member of the Leadership Team). She has been exceptionally helpful and integral to the process by providing advice, guidance, examples, and support. In addition, valuable feedback came from **Emy Tseng, Don Williams**, and **Aimee Meacham** among many others of the National Telecommunications and Information Administration who have contributed to this and preceding, formative work.

The Leadership team would like to acknowledge **Sokwoo Rhee, Ph.D.,** Associate Director of Cyber-Physical Systems at the National Institute of Standards and Technology (NIST), and **Chris Greer**, Senior Executive for Cyber-Physical Systems, National Institute of Standards and Technology. Their insight, leadership, encouragement and support for this Action Cluster and the Global Cities Team Challenge program (from which this Action Cluster was created) have made it an overwhelming success. GCTC's successful model for flexible global collaboration and partnership across all levels of research and education, and government and the private sector has proven itself over time. NIST's guidance on best practice, and future standards, is invaluable for Smart Cities, Communities, Regions and Nations worldwide. The Leadership Team would also like to thank DHS S&T's **Christos Papadopolous** and NSF's **Megan Houghton** for their support and for co-leading the Leadership event.

Finally, the authors and editors acknowledge prior Syracuse University School of Information Studies research and support from NSF grants # 0917973 and #0227879 which led to the insights informing the architecture presented here, and in particular the Open Specification Model v0.5, still evolving five years after NSF Partnerships for Innovation project concluded. Clearly, further research is necessary! :).

Table of Contents

Contents

EXECUTIVE SUMMARY

Purpose

The City of Syracuse is implementing inclusive smart and secure community projects, beginning with a network of city-owned smart streetlights. The cyberphysical smart city architecture guidelines provided here are intended to provide a comprehensive data template for cities of limited resources to apply across sectors and initiatives consistent with NIST standards. The hybrid cloud architecture can include multi-cloud, inter-cloud and federated cloud (to edge) service designs able to support security, confidentiality, access control, least privileges and safeguarding PII practices of data across the Internet of Things and beyond. The 3-level data classification scheme to be considered by City officials and their partners in smart city, community and region projects would define:

1) **Red** sensitive data including personally identifiable information; so most controlled and restricted
2) Yellow medium sensitivity information whose access may be controlled but by law can be shared more widely; although still with controls and monitoring; and
3) Green low sensitivity data which can be shared openly – smart city civic and open data

The purpose of this draft blueprint is to provide readers with a practical guide for deploying a secure cloud architecture for your community, respecting privacy, property, and other human rights. Whether you are a student or researcher, a citizen-scientist, a public official, a municipality, a small or medium business, or an infrastructure, service or technology provider, implementing the simple data classification model presented here is basically the same process. And equally important for improving cyberphysical system security awareness and -better- practices for smart city, community and region-wide privacy and rights-inclusive by design architectures, policies, and processes.

The intent of a secure cloud architecture for open public data is of course to also ensure sensitive personal, corporate, and public service data can be understood and handled with safety. All readers will be able to speak the same simple cloud data classification language after reviewing these guidelines. With the common conceptual understanding of a smart city, community, or region as a cyberphysical system, mechanisms to better coordinate cloud services, including cloud backups for disaster recovery, and reduce costs by use of common templates and models are now something many should feel empowered to participate in the planning of for their community, and help extend the public, social, and economic benefits of smart, secure, private and inclusive by design cloud service innovation and cyberphysical systems growth in your smart city, and beyond.

The goals of the Global City Teams Challenge program are to bring together thought leaders and experts on a wide variety of topics relating to modern “Smart City” technologies and to have them share their knowledge and create best practices to assist those who are coming after them. The authors and contributors of this blueprint have designed, built, and advised the development of secure cloud architectures before. This is intended for readers who may need to consider the challenges and complexity, and also elegant simplicity (compared to most legacy systems) of a Secure Cloud Architecture for smart cities and communities. It is intended for readers at all levels of organizational decision making and influence from elected officials and their executive staff, to community groups, technologists (e.g., information, data and computer scientists and professionals. Engineers, security experts, and IT analysts as well as finance and procurement specialists, marketing, innovation and development specialists, and educators and students of all ages and interests may all find this Blueprint helpful, to begin to speak the same language, and develop common methods and models for community education, self-protection, risk mitigation and most importantly for success – as you help develop, and evolve, your own smart city, community or region-wide cloud privacy security and rights-inclusive architecture.

GCTC CPAC SC3-cpSRIA Secure Cloud Architecture Guidelines

Introduction

The privacy and security challenge for smart cities and communities is multi-faceted and complex. For city managers, workers, community residents and businesses, it can feel overwhelming. Even for technology businesses, and smart building operators, the wide range of legal, social, and technical issues to be considered may feel impossibly muddled and confusing. Part of the problem has been the lack of an overarching smart city cloud and privacy security architecture, to articulate principles and practices at a high level which are nonetheless straightforward and reasonably feasible to be implemented; with a high probability of reducing the range of cyber-vulnerabilities smart cities and their residents, as well as the public, community, and commercial firms operating in the city and on its data - confront daily.

Smart cities run largely on cloud services for efficiency and affordability reasons. Residents, government agencies, and small and medium businesses can benefit from an Architecture or Framework for privacy and rights-inclusive security practices across smart city and community cloud services. First, the City of Syracuse, New York, USA, in cooperation with Syracuse University and SC3-cpSriA Action Cluster(Smart City and Community Challenge Cloud privacy security rights inclusive Architecture) consider how the Architecture guidelines may apply. The SC3-cpSriA Action Cluster welcomes new members to broaden the debate. First, smart streetlight networks, catch basin monitoring, and water metering projects may consider if and how security, privacy, data protection and rights-inclusive cloud architecture guidelines may be followed. The ethics for facial recognition, machine learning and artificial intelligence systems and cloud services in future smart cities with privacy, security and rights-inclusive architecture will also be reviewed.

Can architecture guidelines and security policies help protect citizens rights and encourage growth of smart city open data lakes, encouraging civic engagement and data privacy security and rights-inclusive innovation, entrepreneurship and economic development? Developing a set of security policies as a guideline for your own City, Community, Region, or organization, public or private, is a modern-day requirement, as Hackers remind us all too regularly. But having policies is not enough, implementing the policies within the cloud architecture framework presented here is critical to improve outcomes. Our research and Action Cluster firms suggest using role-based security and storage policies as a way to make the system agile and flexible to adopt new regulations or changes based on new legislative mandate.

This chapter offers guidelines for a smart city privacy and security architecture and a simple, elegant, featuring a smart city data classification schema. Implementation of the architecture can help focus resources on sensitive data in need of protection. It can also enable and encourage wide access to open government data, so that researchers, students, non-profits, start-ups and technology companies supporting the city and the public can dig in and perform their own analyses on civic data. Job creation while building better constituent services are among the objectives of many smart city projects. These guidelines suggest those jobs are more likely to be sustainable if designed to work within NIST standards and best practice recommendations. Several examples being addressed by the City of Syracuse are highlighted in this chapter; as these will be among the first to which application of the guidelines will be applied. Future updates to this chapter will include more information on lessons learned and challenges overcome from these use cases. The Secure Cloud Architecture Action Cluster will offer architectural advice, first on City of Syracuse projects.

1. Smart streetlight network
2. Catch basins
3. Water metering

4. Facial recognition, machine learning and artificial intelligence smart city project policy and ethics

Challenge

"A recent report predicts that by 2018, 20 of the world's largest countries will have in place prioritized national smart city policies, and one third of medium and large cities worldwide will have developed a smart city roadmap." [2]

A lot of data and infrastructure is being deployed and collected in cities with the resulting systems getting more and more complex [2]. These systems of systems need clear and consistent security and privacy requirements and policies. Some of the data collected, and cyberinfrastructure as well as cyberphysical systems (such as IoT) needs to be adequately secured. But not all data is sensitive and applying the same security and privacy policies across data types is wasteful and inefficient.

To solve this a standard, or smart city cloud architecture, is needed which is overarching in its efforts to provide guidelines on privacy and security independent of industry or use case. This framework aims to be provided guidance to municipalities and other smart city implementations in guiding them to a secure and privacy considerate smart city deployment.

Scope

This framework covers considerations to enable security and privacy in smart cities. It does not cover socio-economic considerations of smart cities to determine which projects to pursue (e.g.: job creation) [1]. However, this framework can support the efforts in determining which project to pursue by providing guidelines around the effort required to achieve security and privacy. Additionally, this paper does not cover questions related to interoperability of systems within the system of systems. Other publications cover this topic and it is considered out of scope for this work [2][3][4]. The only consideration made to interoperability is that privacy and security should not inhibit interoperability. While privacy is a key consideration and metrics are introduced here there is additional documentation available that enhances the privacy considerations outlined here [5][6].

Smart City Risks

The rise of smart cities across the world present a new set of risks, some of which are unique to smart cities and some of which are new to the parties overseeing the deployment of smart cities. This chapter will provide a brief overview on how risk is understood in this context and outline a couple of risks associated with smart cities. While the risks outlined here are a good starting point for any smart city to think about risk this list is not comprehensive and smart cities will have to spend additional time and resources in identifying all risks applicable to each smart city project.

Often risk is considered as a formula of Vulnerability (V) times Threat (T) times Consequence (C) ($R = V \times T \times C$) [7]. Vulnerabilities are the weaknesses in a system. On their own vulnerabilities are not a risk. Only when combined with a threat that could misuse the vulnerability and a (negative) consequence does a risk exist. When thinking about risks it is a good approach to begin by listing all potential vulnerabilities to a smart city, as well as the threats that exist to a smart city and potential consequences if a malicious actor was able to get access to a system.

Smart Cities have the potential to enhance every person's life who lives in them. However, Smart Cities also pose a new set of risks which can impact the core of each citizens privacy by collecting data and information on citizens in a scope previously un-seen. Some of the risks that Smart Cities face are:

- Disclosure of Personal Identifiable Information (PII) collected throughout the smart city.

- Unlawful surveillance of citizens by malicious actors or law enforcement.
- Increased area of attack due to deployment of many different systems (cloud, IoT,blockchain and other threats from malicious actors.

This framework will help in identifying the risks and mitigating them in an efficient manner. In addition to this framework readers can also refer to the NIST Cyber Security Framework (CSF) which feeds into the NIST Risk Management Framework (RMF).

Security and Privacy Data Dimensions

When talking about security and privacy it is important to be able to differentiate between the two. Security focuses on preventing unauthorized access, ensuring the confidentiality, integrity and availability of data, systems and infrastructure. Privacy is concerned with the type of data. It provides answers to questions such as: what data should be collected, and how often it should be collected, as well as how often is should be collected, what the permissible uses of the data are, who can the data be shared with, how long should it be retained and the granularity of access control model [8]. Volume of data can impact the performance of the system and may degrade the usefulness of the data and increase cost of system for storing data that may not need to be stored.

City Data Classification Policies

The objective of applying this architecture at a city level is engaging community residents – including businesses of all sizes, local, city, county and state government agencies, and civil society. This will improve the smart city privacy, security, and rights-inclusive operational and policy practices and awareness, while enhancing collaboration, reducing costs and enabling new services. It is anticipated that technologies such as Artificial Intelligence, Augmented Reality, Autonomous Systems, Blockchain, the Internet of Things, Machine Leaning and Quantum Computing may be safely and securely used more widely, while limiting opportunities for personal data abuse by malicious actors. This data classification for smart city cloud to edge architecture will offer a comprehensive approach and easy to use template for organizations to apply their own data classification policy. Eventually it is hoped to extend across all smart city and especially civic data across relevant domains and sectors enhancing personal data rights by design.

Impacts

A smart City architecture to increase privacy security and rights inclusive standards awareness with a simple cloud architecture improving data protection and privacy practices across sectors. Reduced City operating costs and greater regional data transparency increasing service and product innovation and sales is expected to result. With common cloud architecture guidelines ensuring smart community privacy, security and data rights are considered by design, many innovations are emerging. The economic benefits from new personal data revenue streams, new products, jobs, economic growth, exports will contribute to growth of regional tax bases and positively serve energy, health, safety, and environmental objectives including:

- Improving safety and quality of lives
- Community acceptance will be replicated across the United States and adapted in other nations.

Smart City Categories

"'The Smart City can be defined as the integration of data and digital technologies into a strategic approach to sustainability, citizen well-being and economic development.' – Scottish Government, 2014" [2]

Smart City Cloud Data Category Overview

To create a security and rights-inclusive privacy architecture it is important to acknowledge the different types of smart city categories and the importance of privacy and security in each category. The table below lists the different smart city categories and sub-categories and highlights different examples for each type of sub-category [2]. This table is not meant to represent all use-cases of smart cities and will be enhanced as new and relevant use cases are developed and become mature (e.g.: digital identity on the blockchain).

Category/Subcategory	Kind of applications (examples)
Built environment	
Smart home	Home-monitoring and management systems
	Building-monitoring and management systems
	Energy-monitoring and management systems
	Water-monitoring and management systems
	Consumption-monitoring systems
Smart building	Building-monitoring and management systems
	Energy-monitoring and management systems
	Water-monitoring and management systems
Land use and management	Land-use classification systems
	GIS-enabled land mapping
	Smart land-use planning systems
Water and wastewater	
Water collection and management	Weather-forecasting systems
	Systems for geo-spatial mapping of networks
Water distribution	Ghost-pipe detection and management systems
	Water-leakages detection and management systems
	Outage management system
	Real-time hydraulic-modeling water
	Distributions tool
	Water and wastewater SCADA
	Application for geospatial management of water-distribution network
	Quality water monitoring and correcting systems
Water consumption	Online systems for understanding and monitoring water usage
Wastewater management	Plant-monitoring and control systems
	Sewer- lines infrastructure-monitoring and control systems
Waste	
Citizens engagement	Online platform to sell and regain value from products
	Web portal to share and provide information
Collection and segregation	Waste-collection scheduling systems (based on sensors and GPS devices)
	Automated waste-collection systems
Waste disposal	Energy-simulation systems
	Landfill-management systems
	Pollution- and contamination-control systems
Energy	
Energy supply	Demand-response management systems

Category/Subcategory	Kind of applications (examples)
	Energy-simulation systems
	Real-time consumption-monitoring and control systems
	Carbon reporting and management systems
	Energy-service management systems
Energy transmission and distribution	Electric SCADA
	Solutions for substation automation
	Solutions for feeder automation
	Overloading management solutions
	Self-healing grid systems
Energy demand	Electric infrastructure-management systems
	GIS-mapping systems
	Network mapping and consumer-
	Indexing systems
	Smart-streetlights systems
	Large customer profiling solutions
	Energy-service management systems
	Consumption-monitoring systems
Transportation	
Travel demand/consumption	Online services to access to public transport and information
	Bicycle-sharing systems
	Carpooling/car-sharing applications
	Multi-channel citizen services to report
	Maintenance issues
	Cash-less payment systems for multi-modal transportation
	Anonymous people counting systems
Traffic management	GPS-based system for real-time tracking of public transport
	GPS-based vehicle-tracking systems
	Smart-parking systems
	Smart-traffic-lights systems
	Freight ICT services
	Efficient incident-management systems
	Real-time roadway-traffic monitoring and analysis systems
	Video analytics-based scenario simulations systems
Surveillance	Video analytics-based surveillance systems
	Efficient incident-management systems
Education	
Learning outcomes	Education-analytics platforms
	Teacher-performance management systems
	Biometric-identification systems
	Student-performance management systems
Learning and teaching	E-Learning platforms
	Video-conference systems
	Curriculum-management solutions
	Online teacher-training solutions
Service management	Online centralized-admission systems
	Online teacher recruitment

Category/Subcategory	Kind of applications (examples)
	Integrated school-management systems
	Surveillance systems
	GPS-based tracking systems in buses
Health	
Health care systems	Logistic-management systems
	Administrative systems
	Patient-information management systems
	Online patient portals
	Online health portals
Health care delivery	Remote diagnostic and support systems
	Critical decision support systems
	Medical-simulation systems
	Remote monitoring and assistance systems
	Diagnostic-analytics systems
Communication	Internet information portals
	Communication systems
Socio-economic development	
E-Governance	E-Government applications
	Open-data platforms
Social Innovation and Inclusion	Citizen-reporting platform for contacting local authorities
	Social-networking applications
Economy and business	E-Commerce solutions
Public safety, policing, and emergency response	
City surveillance and crime prevention	Mobile emergency services
	Cybersecurity tools
	Incident-control systems
	Surveillance systems
	Integrated response and emergency systems
Communication	Online platforms and services
Prevention and managing of natural disaster	Modelling and simulations in preparation process of crisis management
	Simulations, supporting decision making during the real emergency
Flood monitoring and forecasting	Systems for remotely alerting residents
	Flood-monitoring network

Table 1: Smart City Categories *[2]*

Security and Privacy implications to Smart City Categories

Category/Subcategory	Security/Privacy implications
Built environment	Security: - IoT Device Security Privacy: - Citizen's privacy (behavioral patterns can be deduced from information)
Water and wastewater	Security: - US Infrastructure Security Privacy:
Waste	Security: - CIA of systems to ensure no manipulation of data

Category/Subcategory	Security/Privacy implications
Energy	Security: - US Infrastructure Security Privacy:
Transportation	Security: - Reliability of transportation (not compromised) Privacy: - Travel patterns of individuals
Education	Security: - Surveillance systems to not be compromised by third parties - PII not to be disclosed - Student data to be secured as per FERPA Privacy: - Any student or teacher information
Health	Security: - Systems impacting health of patients Privacy: - Secure patient data in accordance with HIPPA
Socio-economic development	Security: - Secure payment systems - Ensure ID systems Privacy: - Secure customer data in accordance with PCI/other regulations - Ensure privacy of citizen data
Public safety, policing, and emergency response	Security: - Availability in disaster case - Proper use of cybersecurity systems Privacy: - Data from surveillance and communication systems to protect citizens privacy

Table 2: Smart City Security and Privacy Implications by Smart City Category

Security Dimension

Overarching Considerations

When establishing a smart city, it is essential that security and privacy are key parts of the design and implementation rather than afterthoughts. With more and more data being collected and systems becoming more and more complex cyber security incidents are commonplace in today's world [9], [10]. These incidents can be caused by external parties as well as internal actors. A smart city deployment has to consider both threat vectors and adequately protect against both. It is imperative that each smart city deployment practices security by design to ensure a sufficient and acceptable level of security.

Every smart city deployment should create and distribute its own policies and procedures in regard to all aspects of the smart city. The following areas should be covered in a dedicated policy/standards document:

- Data Security/Data Integrity
- Information Security & Assurance
- Identity and Access Management
- Information Security Governance
- Change Management
- Business Continuity / Disaster Recovery

The following high-level steps should be taken by every city, community and region considering a smart city

deployment to ensure security. These steps broadly fall within the 5 functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover [11].

#	NIST Function	Step
1	Identify	Create a data model
2	Identify	Identify and measure risks (assign likelihood, impact and overall risk)
3	Protect	Establish Cybersecurity risk-management Framework and controls
4	Detect	Conduct risk self-assessments
5	Respond/Recover	Continuously improve and enhance controls, risks and smart community security and privacy policies

Table 3: Steps to implement a Smart City with NIST Functions *[11]*

For each one of these steps available standards should be utilized to create a comprehensive security framework. This framework will point out the key standards and regulations where applicable. However, based on the use case and circumstances additional external references might have to be considered.

Create a data model

When considering data collection and types of data available in a smart city it is important to understand the CIA triad as the driver of the creation of a data model. The goal of the data model is to create a basis which can be used to limit exposure to risks to the confidentiality, integrity and availability of the data.

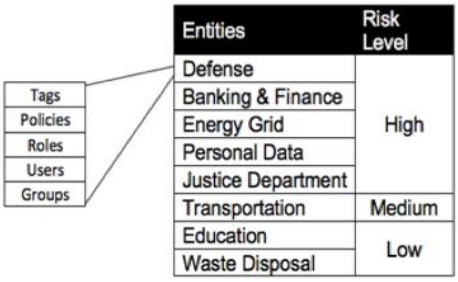

Figure 1: Sample Data Classification [12]

The first step in creating the data model is to identify all data that could be collected. For all data that is identified the type, value, sensitivity and criticality have to be defined [13]. The identification of confidentiality as well as the potential impact of unauthorized disclosure (confidentiality), modification (integrity) and destruction (availability) of data is used to drive the next step in creation of the data model, identifying the minimum amount of data required to operate the smart city.

Once all data has been identified it is important to identify the minimal amount of data required to efficiently and successfully execute the tasks within the smart city. Based on this determination only that data should be collected, processed or otherwise used by any system within the smart city. For all data that has to be collected the flow of data has to be understood and documented. This can help to highlight any regulatory or otherwise legal requirements [13].

To help create easy insight into the different data types and report on what data is being collected it is useful to further group the data and assign it a simple color flag. Data can be grouped into the below categories for reporting and visualization purposes.

Green	Data that can be shared freely (i.e.: Open Data Lake, Civic Data Repository, Open Data Observatories, etc.)
Yellow	Data that can be shared with selected parties • Certain types of PII and other controlled information that may or may not be shared beyond a particular application with permission. • Some of this data could be shared with the permission of the individual from which the data was collected in return for compensation.
Red	Data that cannot be shared • Controlled proprietary information • No automated sharing of data if not by a vetted and approved smart contract. Sharing of data requires explicit approval.

Identify and Measure Risks

As demonstrated above a plethora of smart city use cases exist. Rarely will a city cover all or most of those use cases. To effectively conduct risk management and mitigate the risks to a smart city it is important to identify the specific use case(s) applicable to the entity at hand. Based on the use cases identified risks that correspond to each use case have to be identified. It is important to keep in mind that certain risks can apply to multiple use cases at once.

Once all risks are identified it is important to assign a likelihood, impact and overall rating to each risk. These values are assigned assuming that no effort is made to mitigate the risk. The assumption is that if the risk materializes without any efforts made to mitigate it what would the impact be and how likely is it that the risk would occur. The overall rating is determined based on the likelihood and impact rating. It is also possible to assign numeric values to both impact and likelihood to quantify the risk measures. The below table illustrates a possible matrix to quantify risks.

Likelihood	Almost Certain	Medium	Medium	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	High
		Insignificant	Minor	Moderate	Major	Critical
		Impact				

Table 4: Risk Matrix (Likelihood x Impact)

Cybersecurity Risk-Management Framework and Controls

Once Risks have been identified and quantified controls have to be put in place to mitigate the risks. Development and implementation of controls can be prioritized based on the risk quantification. Where possible, controls should be automated to achieve the most efficiency and impact in mitigating impact and likelihood of each risk.

GCTC CPAC SC3-cpSRIA Secure Cloud Architecture Guidelines

Below are some key control-areas are listed as well as some key controls that should be implemented. While this serves as a baseline for implementing controls the below control areas are not to be seen as comprehensive or all encompassing. Additional controls have to be developed where necessary.

Control Areas
Audit and Accountability
Awareness and Training
Business Continuity Management & Operational Resilience
Change Control & Configuration Management
Data Security and Integrity & Information Lifecycle Management
Governance and Risk Management
Human Resources
Identity & Access Management
Incident Response
Infrastructure & Virtualization Security
Media Protection
Physical and Environmental Protection
Program Management
Security Assessment and Authorization
Security Incident Management, E-Discovery, & Cloud Forensics
System and Communications Protection
System and Services Acquisition
System Maintenance
Threat and Vulnerability Management

Table 5: Control Areas *[13], [14]*

The following controls are select controls considered to be key controls that should be implemented to enable sufficient risk mitigation. These controls alone do not suffice to mitigate all risks to a smart city, community or region. However, without these controls the risks to a smart city cannot be adequately mitigated. To enable the development of the entire controls catalogue smart city deployments should refer to industry standards such as NIST Special Publication 800-53 [14] and the CSA Cloud Controls Matrix [13].

Reference	Control Name	Control Description
NIST 800-53	AC-5 Separation of Duties	**The organization:** a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.
NIST 800-53	AC-6 Least Privilege	**The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users)**

Reference	Control Name	Control Description
		which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
CSA CCM v3.0.1	EKM-04 Encryption & Key Management Storage and Access	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.
CSA CCM v3.0.1	IAM-02 Identity & Access Management Credential Lifecycle / Provision Management	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)

Reference	Control Name	Control Description
		• Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expire able, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements

Table 6: Selective Key Controls *[13], [14]*

Risk Self-Assessment

Using the risks identified and quantified as well as the controls developed each smart city deployment should regularly self-assess their controls as well as their risks. To effectively self-assess a smart city deployment should determine the frequency of the assessment as well as determine the acceptable risk level for each risk assuming effective controls in place. The frequency for assessing each control is determined based on the rating for the underlying risk that is being mitigated by the control. The results of the control assessment should be documented and retained for future needs (e.g.: audits, etc.). Once the controls have been assessed it is important to determine the impact and likelihood for each risk that could have been mitigated by the control. Based on the determination of the remaining risk and the previously established acceptable risk the smart city needs to determine whether or not to accept the remaining risk or if further steps need to be taken (see below for details).

Continuous improvement

If the risk assessment highlights a risk that is not mitigated to an acceptable level by the controls implemented steps need to be taken to improve on the control environment to ensure that the risk is mitigated to an acceptable level. This can be done by either defining and implementing additional controls to close gaps where no control has existed, or existing controls can be enhanced. Enhancements can either be accomplished by updating the control in a way that it covers an area that was previously not covered or by ensuring that the control implementation is operating as intended.

Privacy Dimension

Ensuring privacy and data protection concerns of the public are addressed by design is beneficial not just to the community but also to officials and other stakeholders. As described above privacy is concerned with what data is collected and what it is used for. For this aspect it is important for smart cities to use the data model created above and use the data types identified. Based on those data types and the use cases under consideration a smart city has to decide what legal and regulatory requirements exist around each type of data and how it has to be secured. Additionally, a smart city wants to consider if any of the data collected could compromise a citizen's

privacy or security and treat that data with the highest level of security. Community and non-profit organizations such as the New York Civil Liberties Union, which is participating in the development of this rights-inclusive architecture, as well as the wider public all have critically important contributions to make for civic awareness and community training. Beyond data privacy and protection, a rights-inclusive architecture will also account for the data rights of individuals, as well as other rights-holders such as firms, public agencies, non-profits and technology providers. The IEEE's Fair-Trade Data Initiative may offer helpful guidelines here as well when its work is complete.

Some considerations to be made around privacy is:

- How long should the data be stored?
- Should the data be anonymized?
- Does the data need to be encrypted? Should it be encrypted at storage and/or at rest?
- Are any specific measures necessary to protect the data in storage or at rest?
-

City of Syracuse Examples

There are multiple examples of smart city implementations. There are multiple resources available online which can be used to identify smart city initiatives. For the purposes of illustration this paper uses the city of Syracuse, NY as an example. The city of Syracuse is part of the GCTC Smart City Action Cluster and has multiple different smart city projects which makes it an ideal example for the purposes of this paper. Below are listed 4 example projects that the city of Syracuse outlines in its GCTC Smart city action cluster [15]:

1. Smart streetlight network: Upgrading streetlights will save the city millions annually, interconnect smart grid data access, reduce greenhouse emissions and increase safety.

2. Catch basins: monitoring hard infrastructure with sensors shouldn't create a privacy issue but does indicate that there could be a problem that would then require the city to fix it which previously we might not have known about so we wouldn't have needed to fix it.
3. Water metering: getting access to real-time information on water meters could be helpful for residents to better understand usage of water and if there are leaks in their pipes but also could be invasive if looked at in real time because then the city or others could monitor exactly when the shower is being taken or when someone goes to sleep or when they are out of town.

4. Facial recognition, machine learning and artificial intelligence: facial recognition could help the city to better prevent crime if the city was to monitor specific people to ensure they did not get close to public buildings or schools; but also, could invade privacy and may not be accurate enough to rely on.

5. Smart streetlight network: Upgrading lights will save cities millions annually, interconnect smart grid data access, reduce greenhouse emissions, & increase safety.

6. Catch basins: monitoring hard infrastructure with sensors should not create a privacy issue. Previously a city might not have known there could be a problem, so could not have been expected to repair.

7. Water metering: accessing water meter data could be helpful for residents to better understand usage and if their pipes leak, but also could be invasive if real time information is shared with the city or others, which could monitor exactly when showers are taken or someone goes to sleep, or is out of town.

8. Facial recognition, machine learning and artificial intelligence smart city project policy and ethics: for example, facial recognition could help a city better prevent crime if specific people were monitored to ensure they did not get close to public buildings or schools; but also, could invade privacy, and may not be accurate enough to ethically rely on.

The City of Syracuse is implementing inclusive smart and secure community projects, beginning with a network of city-owned smart streetlights. The cyberphysical smart city architecture guidelines provide a comprehensive template for cities of limited resources to apply across sectors and initiatives consistent with NIST standards. The hybrid cloud architecture includes multi-cloud, inter-cloud and federated cloud (to edge) service designs able to support security, confidentiality, access control, least privileges and safeguarding PII practices of data across the Internet of Things and beyond. The 3-level data classification scheme to be considered would define: 1) sensitive including personally identifiable information so most controlled and restricted (red); 2) medium sensitivity information whose access may be controlled but by law can be shared more widely although still with controls and monitoring (yellow); and 3) low sensitivity data which can be shared openly – smart city civic and open data (green).

KPIs

For 1st Action Cluster project (Advising on smart streetlight network:):

1. $1-$3 Million annual savings from interconnected smart grid data access
2. Reduced greenhouse emissions by 35%, and
3. Increased safety by up to 39% crime reduction at times of smart lighting use

Measurement Methods

1. Annual savings to be calculated by City by same cost accounting methods as used by City in prior calculus justifying purchase of smart streetlights, to derive the $3m annual cost savings number previously projected by the city.
2. Greenhouse emissions to be calculated by difference in energy use required by the new streetlights (when deployed) versus the legacy system.
3. City crime reporting statistics correlated with deployment data on the new smart streetlights and contrasted with prior years data.

Demonstration/Deployment

At the GCTC Expo in July 2019:

- A Proof of Concept for smart city architectural readiness self-evaluation will be demonstrated by WiTec (Syracuse University) and Adaptable Security.

- An illustration of how the City of Syracuse is working with the community and the Action Cluster to refine the privacy, security and rights-inclusive by design smart city cloud architecture for the Syracuse SURGE program, and County-wide, will be presented.
- A Pop-Up community network for Smart City officials use in the event of an emergency, or when in a restricted network access location or dead zone environment. will be simulated. How a NIST and Open Specifications Model 0.5 -compliant Internet Backpack for assured communication on demand always can radically reduce the time to restore communication and more flexibly align emergency services with First Responders and the community, will be shown live.
- A Smart City Data Rights Demonstration will show people claiming rights to their own health data, in conformance also with the Architecture and the Model.
- The Guidelines for Smart City Cloud privacy security and rights-inclusive Architecture will be announced, discussed, and disseminated at the GCTC Expo and Executive Leadership Forum, July 2019, in cooperation with release of the GCTC Cybersecurity and Privacy Advisory Committee (CPAC) Guidebook.
- Los Angeles Unified School District consideration of if and how lessons learned in Syracuse may be potentially applied or adapted has begun; demonstrations and discussions are planned for August 2019.

Future Research on Security, privacy, data protection and rights policies across technologies

- Further extension and refinement of the architecture by vertical/data type will continue and therefore we already know there will need to be an annual update (second edition) to this architecture.
- Meaning the SriA Architecture is not static, and communities must continue to explore the myriad cyberphysical systems dimensions of their smart city opportunities, and threats.

The project will ensure replicability, scalability, and sustainability by continuing to explore conforming to standards including:

- 3GPP/ITU 5G (defined in 2020);
- FEDRAMP;
- FERPA;
- GCTC CPAC Privacy and Security Guidelines;
- GDPR;
- HIPAA;
- IEEE LoRaWAN;
- ISO 37101, Sustainable development and resilience of communities— Management systems — General principles and requirements
- ISO 37120:2014, Sustainable development of communities — Indicators for city services quality of life
- ISO 37150:2014, Smart community infrastructures — Review of existing activities relevant to metrics
- ISO/PWI 37153 Smart community infrastructures
- NIST Framework for Improving Critical Infrastructure Cybersecurity; NIST Smart City Interoperability Reference Architecture (SCIRA);
- NIST SP 800-53; NIST SP 800-171 & NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII);
- NIST A Consensus Framework for Smart City Architectures IES-City Framework (Internet-of-Things-Enabled Smart City Framework) Release v1.0;
- OMB Memorandum 07-16;
- Open Specifications Model 0.5 for the Internet of Things
- PCI
- VMware SDDC & NSX SD-WAN by VeloCloud

Conclusion

These Secure Cloud Architecture Guidelines for smart cities, communities and regions will be refined and extended drawing on criticism and comments, including from initial experience in the City of Syracuse, and then for evaluation of its replicability and generality, by other communities. YOUR community, we suggest, should consider how to apply these guidelines to meet your own needs and requirements, iteratively, over time. Since the threats, and the need, will not stop.

The Smart City and Community cloud privacy, Security and rights-inclusive Architecture guidelines presented here by the GCTC CPAC SC3-cpSriA Action Cluster have shown why and how a cyberphysical smart city architecture guideline can be applied to civic data, open data, as well as private and sensitive data. Whether that data is stored in an Open Date Lake or a municipal system, by a data collaborative, a public agency or a community organization or business, the same framework can be applied to ensure understanding and common data practices respecting rights are followed.[16, 17]

The guidelines provided here provide a comprehensive data template for cities, communities and regions of limited resources to apply across sectors and initiatives consistent with NIST standards. The hybrid cloud architecture presented here can include multi-cloud, inter-cloud and federated cloud (to edge) service designs able to support security, confidentiality, access control, least privileges and safeguarding PII practices of data across the Internet of Things and beyond.

We strongly suggest the 3-level data classification scheme presented here be considered by City officials and their partners in smart city, community and region projects to define:

1) **Red** sensitive data including personally identifiable information; so most controlled and restricted
2) Yellow medium sensitivity information whose access may be controlled but by law can be shared more widely; although still with controls and monitoring; and
3) Green low sensitivity data which can be shared openly – smart city civic and open data

References

[1] ISO, "IST 37129:2014, Sustainable development of communities - Indicators for city services and quality of life", 2014.

[2] IES-City Framework Public Working Group (IES-City), "A Consensus Framework for Smart City Architectures," 2018.

[3] ISO, "ISO/PWI 37153 Smart community infrastructure".

[4] NIST, "NIST Smart City Interoperability Reference Architecture (SCIRA)"

[5] ISO, "ISO 37150:2014, Smart community infrastructures - Review of existing activities relevant to metrics", 2014.

[6] NIST, "NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[7] P. Wong, "Global City Teams Challenege 2019: Smart Secure Cities and Commmunities Challenge (S3) - GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook." 2019.

[8] B. Dean, "Privacy vs. Security," *Secureworks*. [Online]. Available: https://www.secureworks.com/blog/privacy-vs-security. [Accessed: 04-May-2019].

[9] L. Feiner, "Facebook blames 'server configuration change' for its longest outage ever," *CNBC*, 13-Mar-2019. [Online]. Available: https://www.cnbc.com/2019/03/13/facebook-suffers-outage-related-to-core-whatsapp-and-instagram.html.

[10] B. Krebs, "Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years," *KrebsonSecurity*, 21-Mar-2019. [Online]. Available: https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/.

[11] National Institute of Standards and Technolgy, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[12] A. Kalita, B. Alowaidah, H. Belsare, R. Aldarmaki, S. Halikar, "IST 714 Cloud Architecture Fall 2018", *Syracuse University,* 2018.

[13] Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Working Group, "Cloud Controls Matrix v3.0.1," *Cloud Security Alliance*, 2018. .

[14] NIST, "NIST Special Publication 800-53 (Rev. 4)." [Online]. Available: https://nvd.nist.gov/800-53/Rev4. [Accessed: 04-Jul-2019].

[15] S. Edelstein, L. Jensen, L. W. McKnight, Y. S. A. Qadir, "Cloud Privacy and Security Architecture for Smart Communities," *GCTC Action Cluster*, 2019 https://gctc.opencommons.org/Secure_Cloud_Architecture_SC3-cpSriA#Description

[16] IEEE Standards Association, Fair Trade Data Initiative. For more information on development of a standards framework for governing the fair trade of personal and human data, see: https://standards.ieee.org/industry-connections/fair-trade-data-initiative.html

[17] Stefaan Verhulst, Andrew Young, "The Potential and Practice of Data Collaborative for Migration," *Stanford Social Innovation Review*, March 29, 2018. https://ssir.org/articles/entry/the_potential_and_practice_of_data_collaboratives_for_migration#

Developed by: Professor Lee W. McKnight, Syracuse University iSchool (School of Information Studies) and the GCTC SC3 Cloud Privacy Security and Rights-Inclusive Architecture Action Cluster. Views expressed are those of Professor Lee McKnight, and may not be shared by Action Cluster participants, NIST, NTA, DHS or NSF.