iCERT
Industry Council for Emergency Response Technologies

Public Safety Grade Data Centers Evaluation Guidelines Series
Step 1 - Data Center Evaluation in an Era of Industry Disruption

iCERT Cloud Working Group
www.theindustrycouncil.org

iCERT

iCERT – the Industry Council for Emergency Response Technologies - is the exclusive trade association championing commercial public safety response technology providers and related organizations. iCERT improves the public safety ecosystem through ensuring that the needs and views of commercial technology providers are recognized and accommodated by all levels of government, driving continuous technology improvements, education, and helping our members reach their organic and marketplace growth objectives.

Founded by a group of prominent business leaders in December, 2005 originally as the 9-1-1 Industry Alliance, iCERT plays an important role as the voice of commercial public safety companies, wireless carriers, and related vendors on public policy issues impacting 9-1-1 and the emergency response system. iCERT's membership is diverse, and many of its members not only have differing business objectives, they may be direct competitors.

Our members believe that business leaders' expertise can assist public policymakers and government emergency communications professionals as they address complex choices regarding advanced communications technology alternatives in the years ahead. Through advocacy, research, and in coordination with the public sector, iCERT plays a vital role in the development and deployment of emergency response technologies.

Through membership in iCERT, companies can and do:

- Advance public policies that will decrease the cost of doing business in the emergency response sector and create new business opportunities for iCERT's members;
- Conduct research to solve systemic industry problems and promote long term growth across the industry;
- Promote increased sales through direct engagement with public safety stakeholders and prospective customers; and
- Develop industry relationships that facilitate partnerships and alliances in furtherance of corporate goals.

On behalf of iCERT's members, thank you for reviewing this information. We hope that it is of benefit. Comments and questions are always welcome.

Kim Robert Scovill, Executive Director - iCERT

To learn more, or to join iCERT, go to www.theindustrycouncil.org.
To contact iCERT, executivedirector@theindustrycouncil.org

Table of Contents

Contributors

Name	Working Group Role	Company
Don Ferguson	Co-Chair	NGA 911 LLC
Reinhard Ekl	Co-Chair	RapidDeploy
Ed Vea	Member	NGA 911 LLC
Matt Melton	Member	AWS
Paul Tatro	Member	Carbyne
Thomas M Klaban	Member	Winbourne
Jason Brennan	Member	JVCKenwood
Matt Serra	Member	Rave Mobile Safety
Henry Unger	Member	Pulsiam
Mark Woody	Member	Exacom
Richard Zak	Member	Microsoft
Clive Wall	Member	Nice
Chandler Hall	Member	Sentar
Roger Marshall	Member	Comtech
Don Mitchell	Member	NG 911 Services
Jeff Wittek	Member	Motorola
Atul Goyal	Member	T-Mobile
Bill Mertka	Member	Verizon

Introduction[1]

Public safety technology is a complex and ever-changing ecosystem. This iCERT Cloud Working Group paper is part of a continuing series of iCERT publications, webinars, public events, and other efforts intended to provide public safety agencies with guidance for evaluating decisions related to the acquisition, maintenance, and operation of such technologies. To make information more digestible, this and subsequent Working Group papers will focus on just one or two issues related to cloud technologies..

As data center facilities have developed to include virtual as well as physical facilities, this has led to confusion and inertia for Public Safety in general and the 9-1-1 industry in particular, on the adoption of any of the new computing paradigms in their operations. There is often the natural tendency to avoid change and “go with what you know,” even when there is evidence that past solutions are no longer meeting present needs. This includes the weight of stranded capital and legacy investments, especially when securing capital, or even just getting permission for new expenditures, which involves complex or difficult processes. Additionally, gaining an accurate and complete picture of what technologies are currently available can mean a challenging dive into vendors' marketing messages to find the essential value in their offerings (especially as it relates to a particular technical and economic situation).

This paper provides a suggested framework for evaluating the choice between a local on-premises data center facility, or a remote data center (hosted or cloud), based on two criteria: reliability and security. Working from a foundation of these criteria offers public safety agencies a simple method of evaluating a data center to determine its adherence to public safety grade infrastructure regardless of whether it is modeled on cloud computing, remotely hosted, or an on-premises solution.

Although each data center has unique requirements and is incomplete without being interconnected between data centers and users, for brevity, this paper does not include an evaluation of the network’s role in interoperability, performance, and scalability. An analysis of networking will be reserved for a future paper.

Data Center

Data Centers, Networks, and Applications are some of the fundamental building blocks of modern public safety infrastructure. In the broadest sense, a data center is any facility where computing resources are shared by more than one user (a “user” may be one organization, divisions in the same organization, or separate organizations).

[1] This paper represents the collective consensus effort of many iCERT members. Individual members, however, often hold varying, and even opposing points of view on some topics or issues. As an iCERT work product, this effort should be referenced only as iCERT’s point of view, and not be attributed as the position of any particular member.

In a small office, a data center can be a closet with a server, a power strip, and some means (such as a LAN) to connect users. An emergency services data center is one that serves some public safety capacity. The server closet in a sheriff's department that might service the jail, office administration, call handling, dispatch, and evidence storage is one example.

Another example is a data center set up by a larger community, such as a major city, region, or state that serves a combination of public safety agencies and other municipal or government clients. Still others are third-party centers shared by both commercial and government users. In recent years more and more data center functions are actually in the "cloud" which, for these purposes, can be thought of as just another form of a shared data center.

Data centers have always been important, but with the convergence of communications and IT, that importance is dramatically increasing. Data centers today are the repositories and enablers of Next Generation 9-1-1 (NG9-1-1), Artificial Intelligence (AI), Big Data, location technologies, communications networks, Computer-Aided Dispatch (CAD), cloud-based systems, public safety broadband wireless networks, Land Mobile Radio (LMR) systems, recording, and cybersecurity.

Whether small or large, dedicated or shared, a functional data center fundamentally provides:

- Computing
- Storage
- Electrical Power
- Interconnection Network[2]
- Environmental Controls
- Security

Data centers have only as much utility as they have secure connections to communications networks and computational and storage resources from which they can serve up information and applications. For public safety, the current Next Generation communications network design for public safety is an Emergency Services IP Network (ESInet). An ESInet, although it may be deployed on public telecommunications networks, must be logically isolated from other traffic through the use of encryption and border gateway functions. Built into an ESInet's design are certain security restrictions that deal specifically with network access by authorized personnel, uses, and network elements.

[2] Interconnected networks introduce increased risk. In the case of public safety, the core network responsible for processing calls in an NG9-1-1 environment, the Emergency Services IP network (ESInet), must be interconnected to both OSPs and Public Safety Answering Points (PSAP). ESInets are protected by security measures and technologies intended to protect them from breach and misuse. These mechanisms increase the trust necessary for implementing interconnected networks.

The “Cloud”

The introduction of resource virtualization has radically altered the landscape of data center technologies, which now include virtual servers and storage technology (what is generically called the “cloud” or “cloud services”) in addition to traditional physical components. Virtualization has driven the widespread availability of cloud computing[3] services like Infrastructure as a Service[4] (IaaS), Platform as a Service[5] (PaaS), and Software as a Service[6] (SaaS).

Emergency Services Networks

The internet formally began in 1981. The ESInet is a derivative of the internet with strong emphasis on security and availability. The ESInet’s heritage specifically dates to RFC 791[7] in September of 1981. RFC 791 defined Internet Protocol (IP). From IP several higher-level applications like File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP), Dynamic Host Configuration Protocol (DHCP), and Session Initiation Protocol (SIP) evolved. These higher level applications, rooted in RFC 791, have provided the foundation for the modern day ESInet.

---

[3] The NIST Definition of **Cloud Computing** https://csrc.nist.gov/publications/detail/sp/800-145/final Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

[4] **Infrastructure as a service** (**IaaS**) The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final

[5] **Platform as a Service (PaaS)** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final

[6] **Software as a service (SaaS)** The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final

[7] INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981 https://tools.ietf.org/html/rfc791

Modern networks that provide end-to-end emergency services have changed radically since 1981. Today's IP-protocol-based networks are usually comprised of three different domains: origination network, emergency services network, and termination network, each having its own relevant reliability target for measurement. Each domain is also represented by its own data center architecture, whether constructed of physical facilities, local, remote or virtual (cloud) facilities, or a hybrid (a combination of one or more of any of these network types).

In the world of end state Next Generation 9-1-1 (NG9-1-1), all 9-1-1 data centers are interconnected to save lives. Unlike email or web surfing, 9-1-1 is a very different service, so while both services utilize various different technologies developed within the RFC 791 protocol family, they have substantially different value to their users: 9-1-1 saves lives, while email and web surfing enhance the quality of life.

In end state NG9-1-1, every 9-1-1 data center is ultimately interconnected with every Originating Service Provider (OSP). In order to achieve a high level of service reliability, the performance of an NG9-1-1 system as a whole should be measured. It is dependent on the various networks between end users and the Public Safety Answering Points (PSAP), including the 9-1-1 data center, and must be well understood and measurable to the extent possible. System performance, with a focus on the relevant networks, is a future topic for this iCERT Working Group and is not addressed in this paper.

Availability

On-premises computer power and storage alone can be subject to practical and financial limits in regards to achieving the highest reliability levels. As a result of these constraints facing premises-based systems, remotely hosted services may offer a realistic alternative, providing computer power/storage, cost-effectiveness, and reliability all at the same time.

The assumed standard uptime for any "public safety" grade service is 99.999% availability.[8] It is important to note that this availability figure refers to system availability as a whole and not simply the data center hardware. NG9-1-1, as a service, is dependent on both hardware and software, but especially the software. NG9-1-1 availability is derived from standard data center hardware running well-architected software with high availability. That means less than just under six minutes of downtime every year. Achieving long term availability equal to or exceeding "five-nines" depends upon aspects of both design and operation. Data center designers acknowledge that a single data center may not be able to achieve five-nines over an extended period of time for the NG9-1-1 service due to unplanned events that may take the data center offline (e.g., earthquake). This leads to the common design choice of multiple data centers in all use cases. The total number of data centers that make up a data center complex can vary, but

[8] *Defining Public Safety Grade Systems and Facilities Final Report,* 5/22/2014, National Public Safety Telecommunications Council (NPSTC). http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf

typically the design is two data centers that are geographically diverse, established on opposite sides of major known earthquake fault lines (for services that are made available at a national or multi-regional level; for smaller-community level deployments, this earthquake fault line design criteria may not be achievable and service availability will be dependent on other design and operation considerations). These data centers should also conform to best practices in interconnection route diversity and redundancy (i.e., multiple ingress and egress connections and/or carriers). In short, to better assure high availability, multiple diverse data centers working in tandem in an active-active configuration is the preferred design as part of a broader data center solution.

Data center availability is based on an overall system design built from individual computer and network components. The overall reliability calculation required to derive an availability value is the sum of the individually calculated reliability for each component that makes up the complete system.[9] To compare reliability between data centers, you need to measure both MTBF (Mean Time Between Failures) and MTTR (Mean Time To Recovery) and use these as inputs to convert to an availability number.[10] It is crucial to understand and compare both of these quantities. For example, a data center could experience daily MTBF, but if the MTTR is milliseconds, then these failures may go largely unnoticed. On the other hand, a data center could experience a yearly impairment (i.e., high MTBF), but if the failure (MTTR) lasted more than six minutes, then the data center would not be considered “public safety grade.”

Security

Security has a direct impact on reliability.[11] An unsecured data center lends itself to compromise, and, when compromised, would most likely be rendered useless or at the least unreliable and untrustworthy. Any data center, no matter how well designed, is susceptible to such vulnerabilities.

The topic of security includes many considerations: acquisition, assessment, asset management, audit and accountability, awareness training and education, compliance, configuration management, contingency planning, incident response, maintenance, media protection, patch management, personnel security, physical and environmental protection, planning, program management, security automation, security monitoring, and cyber threat hunting. Due to its complexity, this paper does not explore security concerns, except to identify the need for 9-1-1 data centers to be extremely attentive to the issue. This topic will be reserved for a future paper.

---

[9] For purposes of this illustration, we’re talking about one system’s components; adding a redundant system, which then makes the “system” as reliable as possible, is not included.
[10] See Reliability Section, below, for more information about MTBF and MTTR.
[11] Security means both physical and electronic (communication) security, and an on-premises versus remote data center would have differing security profiles. For purposes of this section, we will focus on network security (e.g., unauthorized access, hacking, etc.).

Challenge: Industry Disruption

NG9-1-1 service implementers are many times hamstrung in moving forward by the public safety industry's current period of technology disruption. Change is rapid, things are unsettled, and no one has a "crystal ball" capable of predicting the future, making it challenging to ascertain WHICH modern technology innovations might help actualize the promised benefits of NG9-1-1.

Cloud computing, AI, and the Internet of Things (IoT) are all modern disruptive technologies that seem, on the surface, to have direct impacts on the public safety ecosystem, but HOW they might positively impact the sector is hard to see in detail at this time.

A complementary disruptive fact is that some public safety agencies have already made substantial capital investments in data center infrastructure.[12] Also, because major network system technology procurement may not be a common occurrence, or previous decisions were made by outside consultants, many agencies lack in-house knowledge and expertise regarding some of the newer trends and capabilities of high availability computing. An unfortunate symptom of this condition is that far too many public safety data centers (especially on-premises data centers) do not satisfy the 99.999%[13] availability objective set forth by the National Public Safety Telecommunications Council (NPSTC), and therefore, are not technically public safety grade.

One particular disruptive technology, cloud computing, has been introduced recently into the public safety ecosystem, creating opportunities for public safety agencies to potentially reduce the complexity and costs of their data center computing infrastructures. However, many public safety agencies do not have a proven procurement method to obtain cloud services for public safety.

The remainder of this paper focuses on managing the disruption introduced by cloud computing and its impact on the historic "concept" of the public safety data center.

Traditional Data Centers

The traditional, on-premises, data center has been a fixture in the public safety industry—long before the availability of remotely hosted services or the advent of cloud services. Older **traditional 9-1-1** solutions have often been implemented in an on-premises standalone data

[12] This comment references on-premises capital equipment; for example, a jurisdiction that has purchased the computing equipment, software, and call center hardware for its operations, including, what this paper would classify, as the relevant supporting "data center(s)."
[13] NENA Emergency Services IP Network Design Information Document, https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-INF-016.2-2018_ESIND_20.pdf

center (everything in one location at or near the PSAP's physical location), and sometimes were managed by the area's primary Local Exchange Carrier. These more traditional in-house data centers were able to take advantage of the proliferation of low-cost computing hardware that began in the early 2000s, making local operational independence and sophistication a reality for many public safety agencies. In contrast, due to its emphasis on networking, economies of scale, and distributed/shared systems, many **NG9-1-1** systems are deployed as remotely hosted installations.

Cloud Computing Arrives

When Amazon Web Services (AWS) was launched in 2006, cloud computing, a service and process distinct from remotely hosted computing, emerged in the general market as a viable alternative to building a traditional data center. Before long, vendors including Microsoft, Google, IBM, and Oracle introduced cloud platforms to serve both private and public sector customers.

One distinction between cloud computing and simple remotely hosted computing is that cloud computing allows users to "rent" virtual, on-demand computing power that can scale server capacity to the desired need quickly and efficiently allowing users to pay only for the capacity actually used. By 2011, the importance and high relevance of cloud computing compelled the National Institute of Standards and Technology (NIST) to establish a standard definition of cloud computing.[14]

What Really Matters

Reliability and security are paramount concerns for public safety agencies regardless if the solution is delivered using cloud computing, a remotely hosted solution, or on-premises infrastructure. In many cases, each of these competing architectures can be offered as a "managed service," and as such, are expected to work reliably with continual support via a Service Level Agreement (SLA). Since an on-premises infrastructure is the trusted incumbent architecture, a disruptive technology like cloud computing must demonstrate compelling advantages in facilitating capabilities, performance, reliability, security, and cost.

[14] The National Institute of Standards and Technology (NIST), "Definition of cloud computing", September 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final

Data Center Tier Classification Standards

The Uptime Institute[15] provides a trusted and accepted standard for the proper design, build, and operation of data centers. The Institute's standard establishes four distinctive definitions of data center site infrastructure: Tier I, Tier II, Tier III, and Tier IV[16], for a single geographic location. These classifications establish a basis for understanding data center conformance to the requirements of public safety grade infrastructure.

The Uptime Institute provides the following tier summary requirements as part of its D*ata Center Site Infrastructure Tier Standard*:

	Tier I	Tier II	Tier III	Tier IV
Minimum Capacity Components to Support the IT Load	N	N+1	N+1	2N+1
Distribution Paths - Electrical Power Backbone	1	1	1 Active 1 Alternate	2 Simultaneously Active
Critical Power Distribution	1	1	2 Simultaneously Active	2 Simultaneously Active
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerance	No	No	No	Yes
Compartmentalization	No	No	No	Yes
Continuous Cooling	No	No	No	Yes

Tier I: Basic Site

If a data center is not completely redundant at every component, then it is a Basic Site. A Basic Site is characterized by a dedicated area for Information Technology (IT), Uninterruptible Power Supply (UPS), dedicated cooling equipment, and on-site generator or fuel cell.

[15] www.uptimeinstitute.com
[16] Uptime Institute Tier Data Centers https://uptimeinstitute.com/tiers

Tier II: Redundant Site

The difference between the Tier I Basic and Tier II Redundant Site is that the Tier II Redundant Site is termed “redundant” because it has a backup on-site electrical generator or fuel cell, UPS, cooling, and extended fuel supply for the electrical generator. A minimum of 12-hours of on-site fuel storage is necessary to achieve this Tier II rating. Also, even though a Redundant Site is Tier II, it should be noted that this remains a single, non-physically redundant infrastructure design; there is only one data center location.

Tier III: Concurrently Maintainable Site

Tier III begins to enter the level of computational processing redundancy that 9-1-1 data centers require, but falls short of public safety grade infrastructure. Above and beyond the Tier II Redundant Site, Tier III level data centers feature redundant components that can handle production level capacity. Additionally, Tier III data centers have multiple independent communications paths.

With a Tier III data center, each and every component can be removed from service without impacting the critical environment. There should be no planned outages at the Tier III level data center since redundant components can handle production loads while components are replaced or repaired. Furthermore, there is sufficient capacity in the redundant components to serve the entire system.

It is worth noting that unplanned catastrophic natural disasters (or man-made) events can still take down a single geographic Tier III data center.

Tier IV: Fault Tolerant Site

The Tier IV, Fault Tolerant Site, is designed to handle unplanned events. Unplanned events include, for example, a cyberattack, major fire, earthquake, flood or volcanic eruption. Tier IV rises to its highest reliability level when paired as a geo-redundant data center facility as even a Tier IV data center is only capable of handling a single unplanned event at a time.

A Tier IV data center complex must be capable of detection, isolation, and containment of any reasonable potential fault. Tier IV data center facilities are the conceptual basis of commercial cloud offerings and should be the foundation of any remote hosted SaaS offering.

By way of example, for planning, the statistically relevant causes of unplanned service outage are:[17]

[17] https://lifelinedatacenters.com/reliability/data-center-downtime/data-center-outages/

- Data center power outage, (UPS failures are 25%)
- Cybercrime (22%)
- Weather (10%)
- Generators (6%)
- Human error (22%) (ill-planned changes made by administrators)
- Other (15%)

Even so, most unplanned IT service outages are preventable or avoidable with sufficient professional planning.

Availability Measurement

Setting aside all the hyperbole surrounding the “newest” and “most innovative” approaches to technology, the reality is that availability is paramount for public safety. To qualify as “public safety grade,” 9-1-1 service must experience no more than six minutes of downtime per year, or 99.999% uptime in any continuous 12-month period.

Highly available systems are designed to manage failure rather than hope failures do not happen. Availability measurements depend upon the quantities Mean Time Between Failures (MTBF) and Mean Time To Recovery (MTTR) (also discussed above). In general, SYSTEM AVAILABILITY = (MTBF)/(MTBF+MTTR). Each of these is a time measurement, so availability is therefore expressed as a percentage.

Mean Time Between Failures (MTBF)

Mean Time Between Failures is the average time elapsed from one failure to the next. MTBF is a critical marker in reliability / availability engineering and has its roots in the aviation industry, where even a minor airplane component or system failure can result in a fatal crash. For critical systems such as 9-1-1 systems, MTBF is an important indicator of expected performance.

Mean Time To Recovery (MTTR)

Mean Time To Recovery is a measure of the time between the point at which the failure is first discovered until the point at which the equipment returns to normal operation. In addition to repair time, testing, and return to normal operating condition, MTTR captures failure notification time and diagnosis.

While MTTR should be included in all Service Level Agreements (SLAs) and maintenance contracts, in general, the lower tier of the data center, the greater the MTTR.

Security Considerations

As mentioned earlier, although this paper does not directly address the security concerns and selection criteria incumbent upon public safety data centers, it does recommend vigilance, study and attentiveness to security issues. The iCERT Cloud Working Group will deal with security criteria in a future paper, but until that is released, the following material is given, not as specific security requirements to follow, but rather as material for consideration, study and familiarization.

NIST Cybersecurity Framework

A Tier IV level data center is “fault tolerant” and can withstand a single unplanned event. A cyberattack is an example of a significant unanticipated event that impacts data center uptimes, and they are, unfortunately, on the rise.

The National Institute of Standards and Technology (NIST)[18], through a collaborative process of industry, academia, and government stakeholders, developed an outline and process for improving critical infrastructure cybersecurity, entitled *Framework for Improving Critical Infrastructure Cybersecurity* (“*Cybersecurity Framework*”).

The five **functions** of the *Cybersecurity Framework* are:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Under these overarching functions, the *Cybersecurity Framework* provides a catalog of outcomes based on existing standards, guidelines, and practices that organizations can customize to better manage and reduce their cybersecurity risk.

The *Cybersecurity Framework* consists of three **components**:

1. Core: provides an easy-to-understand set of desired cybersecurity outcomes.
2. Profiles: portrays organizations’ unique requirements, objectives, risk appetite, and resources.
3. Implementation Tiers: indicates how an organization manages cybersecurity risks.

[18] https://www.nist.gov/

The Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual, organizational Profiles. Through the use of Profiles, the *Cybersecurity Framework* will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Implementation Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.[19]

The *Cybersecurity Framework* provides a valuable and uniform approach (across companies and industries) to prioritize cybersecurity resources, make risk decisions, and take action to reduce current and future risks. It enhances cybersecurity communication within an organization and with other organizations (such as partners, ESInet and NGCS providers, 9-1-1 Authorities, and OSPs), and helps organizations identify, manage, and assess cybersecurity risks. This framework helps manage the complexities of cybersecurity through an approach that addresses how organizations ought to identify, detect, protect, respond, and recover - all with relation to cybersecurity.

Cyberattacks

Cyberattacks account for a significant percentage of unplanned outages, so the deployment, maintenance, and operation of cybersecurity systems are a necessary component of every data center.

The federal government recognized the threat of cyberattack long ago and has made significant investments to thwart cyberattacks on its communications facilities and data centers. These standards and best practices are embodied in the work of the NIST *Cybersecurity Framework* previously discussed.

This Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.[20]

Each 9-1-1 Authority should first ask, "When was the last security audit?", then ask a follow-up question, "Does my security audit demonstrate that the NIST *Cybersecurity Framework* is implemented in my organization and data center?"

[19] NIST Cybersecurity Framework https://www.nist.gov/cyberframework
[20] NIST Cybersecurity Framework https://www.nist.gov/cyberframework

Cloud Security Alliance

While the *Cybersecurity Framework* can be applied to all organizations, there is also a security measurement framework specific to cloud solution providers. The Cloud Security Alliance[21], a not-for-profit organization with a mission to promote security assurance within cloud computing best practices, publishes a technical controls document specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The document, *The Cloud Controls Matrix* (CCM)[22] is a unified controls document covering 13 different compliance frameworks across 16 different technical and procedural disciplines. It is specific to cloud environments.

Criminal Justice Information Systems (CJIS) Compliance

Law enforcement and other government agencies in the United States must ensure that their data centers which transmit, store, or process Criminal Justice Information (CJI) comply with their own version of security measurement, the Federal Bureau of Investigation (FBI) CJIS Security Policy which establishes the minimum security requirements and controls to safeguard CJI[23].

Private companies that process CJI must sign the CJIS Security Addendum,[24] a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the CJIS Security Policy. It also commits the signatory to maintaining a security program and controls consistent with federal and state laws, regulations, and standards, including the CJIS Security Policy.

Federal Risk and Authorization Management Program (FedRAMP)

The federal government has created the Federal Risk and Authorization Management Program (FedRAMP),[25] to ensure conformance with cybersecurity standards and practices. FedRAMP is an assessment and authorization process that U.S. federal agencies are required to use when procuring cloud solutions. It consists of a subset of NIST Special Publication 800-53[26] security controls, which are the basis for much of the NIST *Cybersecurity Framework* (discussed above). Those controls were specifically selected to provide protection in cloud environments. A subset

[21] https://cloudsecurityalliance.org/
[22] https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview
[23] DOJ CJIS Security Policy
https://www.fbi.gov/file-repository/cjis-security-policy_v5-7_20180816.pdf/view
[24] http://www.bidnet.com/bneattachments?/373987147.pdf
[25] https://www.fedramp.gov/
[26] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

has been defined for the Federal Information Processing Standard (FIPS) 199 low categorization and the FIPS 199 moderate categorization.[27]

The FedRAMP program has also established a Joint Authorization Board (JAB) consisting of Chief Information Officers from DoD, DHS, and GSA that issue authorizations to operate (ATO) for applying cloud solution providers.[28] FedRAMP is seen by most as the “high water mark” of cybersecurity compliance. While not required for public safety, FedRAMP approval may be beneficial for certain cloud environments over time. Cloud solution providers such as AWS and Microsoft Azure hold FedRAMP ATOs.

[27] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[28] https://www.fedramp.gov/jab-authorization/

Cloud Compared to On-Premises

What type of infrastructure path should public safety agencies take in the era of cloud computing? Is some variation of a cloud-based infrastructure the way to go, or should agencies stick with the tried and true on-premises solution?

The decision made will depend upon first understanding the current system infrastructure and then making transformation/upgrade decisions based upon each agency's unique requirements. While each agency/Authority will ultimately make its own decision, the following matrix is provided to allow for a quick comparison between the characteristics and strengths/weaknesses of adopting either path.

Evaluation Matrix

	Cloud	**On-Premises**
Available Tiers	Tier I, Tier II, Tier III, or Tier IV data center	Tier I, Tier II, Tier III, or Tier IV data center
Tier Selection for Public Safety Grade	Includes only Tier III+	Tier selection based on available budget
Infrastructure	1) Minimal, if any, additional on-premises hardware/software 2) Flexible architectural design 3) easily-expandable capacity (potential natural disaster exception) 4) Actual demand/usage drives costs and other processes	1) Unique hardware-specific solution 2) Relatively fixed architectural design 3) Maximum capacity-based design 4) Assumed capacity drives costs and other processes
Network Security	1) Centralized at the Cloud Data Center 2) Shared resource 3) Audited, tightly controlled, highly collaborative, and real-time	1) On-site security team personnel 2) 24/7 resource scheduling, and requirement to maintain 3) Commitment to ongoing equipment specific training
Service Level Agreement	1) 99.95% offered; 99.999	1) SLA set in agreement

Uptime Percentage	available, but requires additional engineering	
Initial Investment	1) Subscription agreement for cloud services 2) Network connectivity	1) All equipment must be purchased in advance of deployment. 2) Facilities, hardware, software, installation, and maintenance
Ongoing Operational Costs	Costs are based on a subscription model and distributed over a broad set of resources.	Costs are aggregated based on individual network,hardware and software maintenance fees plus periodic upgrade costs and operational resource team costs.
Time to Implement	1) Design & Planning (establish outputs) 2) No significant on-premises activities 3) Network connectivity time frame 4) In general, shorter.[29]	1) Design & Planning (establish inputs, processing, personnel, and outputs) 2) Detailed on-premises installation 3) Some or reduced connectivity time frame 4) In general, longer.[30]
Infrastructure Scaling	Equipment capacity is dynamically scalable as an automatic part of the service design.	On-premises environments require advance capacity planning to create scalability.
Change Management	Upgrades are a shared resource among many users, and can progress independently of any one user's resources.	Cyclical upgrades designed and executed only by and for the organization with its resources.

Hybrid Cloud

Hybrid cloud is another optional "flavor" or model of cloud computing that combines elements of on-premises and cloud computing to provide additional flexibility and options. For example, in a hybrid cloud deployment, an agency can choose to store its data on-premises, but run its

[29] *See* discussion of Agile Project Management, below
[30] See discussion of the Waterfall Model, below.

applications in the cloud. Another hybrid cloud capability is running some cloud-only solutions using an agency's own IT infrastructure (e.g., supporting remote sites with limited network connectivity).

It is worth noting that in a Hybrid Cloud architecture reliability can depend on the data centers that are interconnected.

Determining the Current Data Center Tier Environment

Regardless if the convenience of cloud, control of on-premises, or flexibility of hybrid cloud is applicable, a public safety organization should first determine its data center's current operational Tier. Next, the organization should establish an inventory of existing infrastructure and compare it to the Tier discussion above to determine if the existing infrastructure deployment matches a Tier I, Tier II, Tier III, or Tier IV data center. Such an evaluation will help establish realistic SLA expectations and allow for monitoring to ensure that the contractual obligations of the SLA are being met (and potentially, why or why not).

Saving Money While Upgrading Tiers

Traditionally, 9-1-1 authorities have looked to their service providers to deliver higher tiered services at a competitive rate compared to other architectures. It is essential that public safety explore all options when evaluating their data center requirements to ensure they can move forward into NG9-1-1 products and services, without cost constraints or the inflexibility of legacy infrastructure. Given the economies of scale and competitiveness of a market based cloud computing ecosystem, it is not unrealistic to expect that public safety can achieve a higher tier service for equal or lesser cost with a cloud-based infrastructure.

Cost Comparison

Research, technical education, and training are required for 9-1-1 Authorities to fully comprehend and respond to questions regarding the following topics:

1. current infrastructure
2. the true actual "total" cost of service
3. how to take advantage of readily available cloud infrastructure
4. how to blend current infrastructure with the cloud

9-1-1 Authorities often use a Managed Service approach to their on-premises facilities, so savings are determined by the alternative service being compared to the cost of these managed services and additional on-premises personnel costs. The internal cost savings of moving to the cloud may not be readily apparent. However, the cloud approach to infrastructure is entirely new to 9-1-1 so it may be a challenge to align the infrastructure to deliver an immediate financial benefit for the 9-1-1 Authority. However, cloud-based service providers are now offering enhanced infrastructure, which should be competitively priced.

It could be argued that by using a cloud architecture, public safety should expect substantially more infrastructure for less money. It is not only the idea that this “bill” will be lower; but also that the total cost of ownership may be lower than legacy methods that require public safety to service and support their own infrastructure.

Service Level Agreement

Establishment of a Service Level Agreement (SLA) is a best practice for both cloud and on-premise infrastructure arrangements. In addition, an SLA is also a requirements document containing terms and conditions for the contracted service. . However, an SLA is only as good as the infrastructure that the contracted solution is built on. So, while a service provider may contractually obligate themselves to a “public safety grade” SLA requirement, unless for example, the infrastructure includes geo-diverse data centers, then a 9-1-1 authority might not realize the performance that they expect to achieve.

Initial Cost

While it is touted that there are no initial capital costs with cloud computing since it’s a service, it is more accurate to note that this may be the case for some planning activities, such as on-premises infrastructure planning sessions to ensure correct capital procurement. While some cloud deployments will necessitate an initial investment to stand the service up, in general, the capital outlays to stand up a cloud-based deployment are usually less than an on-premises deployment.

Other considerations include the costs for adequately sized secure network connections, given minimal on-premises hardware and IT support. Note that if quality network connectivity already exists, this may only be an upgrade or reconfiguration.

In contrast, an initial on-premises infrastructure project requires that all the capital costs associated with building a data center are incurred before the system can be declared operational. These cost elements include servers, hardware, software, data backup, storage, disaster recovery, remote access, and (internal and/or external) network connectivity. . In general, on-premises deployments have higher initial capital outlays than cloud-based deployments

Recurring Monthly Costs

There are ongoing costs in both cloud and on-premises infrastructure scenarios; software upgrades, technical support, and consulting remains necessary regardless of the data center tier or deployment infrastructure choice. However, both scenarios provide the opportunity to negotiate relevant and appropriate service levels and pricing.

Infrastructure Rightsizing

For comparison to existing and proposed vendor solutions, 9-1-1 Authorities should conduct studies of:

1. existing legacy infrastructure (even if provided remotely) to determine:
    a. what standard and peak capacity is available
    b. how available (and sustainable) the peak capacity is
    c. how efficiently the solutions are utilized
2. MTBF statistics
3. MTTR statistics

In the past, on-premises pre-production capacity decisions could lead to over-capitalizing or under-capitalizing the project with the resulting under or over resourcing of facilities and throughput. Proper engineering should be done to avoid over or under capitalizing the project.

With cloud computing, 9-1-1 Authorities can access as much or as little capacity as needed, and quickly scale up and down as required. Having the ability to more rapidly scale necessary infrastructure than was possible in the past can be a critical factor for 9-1-1 operations when handling large scale emergencies, for example, a car accident in a busy metropolitan area, active shooter situations or severe weather. Another example is adding a permanent or even temporary call-taking position.

Conclusion

Traditional, on-premises deployment architectures may lead many public safety agencies to assume that it is unnecessary to periodically evaluate leveraging cloud-based infrastructure and related applications. This is an understandable yet inevitable constraint of operating critical, mandated infrastructure on a tight budget within a vendor community that may be slow to introduce needed innovation to the sector due to these fiscal constraints. A near-universal “this is how we’ve always done it” mentality has also remained the comfortable norm in the sector over the years. However, today’s technology revolution, which has resulted in NG9-1-1 and a host of other cloud-infused advanced public safety technologies, has made the current state of affairs unnecessary, if not untenable.

Based on the results of the audits discussed above, many, if not most, public safety agencies may conclude that their current data center resource deployments are over- or under-capitalized. Employing some flavor of cloud-based resources can offer new opportunity because cloud-based infrastructure and applications have shown they can solve many of the problems facing public safety technology deployment today, despite the cost of disruption to existing operational and procurement procedures.

Nevertheless, judicious and appropriate use of cloud resources promises quicker deployment, easier continuous improvement, and better scalability, reliability, security, and use of scarce technology funds for public safety. All of this is dependent, of course, on solid agency work in specifying individual services requirements for each jurisdiction and then basing infrastructure and applications acquisitions on those requirements.

The potential advantage of any change requires an accurate quantitative and qualitative assessment of your current operational metrics, potential, and costs. It’s recommended that a 9-1-1 Authority starts with an inventory of what is “under the hood” of your data center(s).

1. Use the “Tier Summary Requirements” to rate your data center as Tier I, Tier II, Tier III, or Tier IV.
2. Rate interconnected data centers.
3. Reconcile your data center’s Tier with your SLAs.
4. Reconcile the SLAs of your interconnected data centers.
5. Conduct a security audit of your data center.
6. Conduct a security audit of your interconnected data centers.
7. Conduct a capacity utilization study of your existing architecture.
8. Reconcile your security protocols with the NIST Cybersecurity Framework.

After an empirical study, an agency will know where they stand. Then they can determine where they are in relation to a public safety grade data center, and what the best course of action

should be. This time around, the vendor community appears to be in a better position to supply the solutions necessary to realize the promise of NG9-1-1 and the cloud is a huge part of the new solutions available from the vendor community.

Glossary

9-1-1 Authority A State, County, Regional or other governmental entity responsible for 9-1-1 service operations. For example, this could be a county/parish or city government, a special 9-1-1 or Emergency Communications District, a Council of Governments or other similar body. [31]

Artificial Intelligence (AI) In computer science, artificial intelligence , sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and animals. Computer science defines AI research as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. Colloquially, the term is used to describe machines that mimic "cognitive" functions that humans associate with other human minds, such as "learning" and "problem-solving."[32]

Big Data Big Data refers to the inability of traditional data architectures to efficiently handle the new datasets. Characteristics of Big Data that force new architectures are: Volume (i.e., the size of the dataset); Variety (i.e., data from multiple repositories, domains, or types); Velocity (i.e., rate of flow); and Variability (i.e., the change in other characteristics). [33]

Computer Aided Dispatch (CAD) A computer-based system, which aids PSAP Telecommunicators by automating selected dispatching and record keeping activities.

Cloud Computing/Cloud-Based Systems Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.[34]

Cybersecurity Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of

---

[31] NENA Master Glossary Of 9-1-1 Terminology https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-ADM-000.22-2018_FINAL_2.pdf
[32] https://en.wikipedia.org/wiki/Artificial_intelligence
[33] NIST Big Data Interoperability Framework: Volume 1, Definitions https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf
[34] The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final

growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.[35]

Cyber Threat Hunting is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.[36]

Dispatch/Dispatching in the context of this paper is a shorthand term used for the assessment of the nature of an emergency request for assistance, and the provisioning of assistance (e.g., police, fire, or emergency medical services (EMS)).[37]

Emergency Services IP Network (ESInet) A managed IP network that is used for emergency services communications, and which can be shared by all (relevant) public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG9-1-1 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network.[38]

Infrastructure as a service (IaaS) The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).[39]

Internet of Things (IoT) The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.[40]

---

[35] Department of Homeland Security, https://www.dhs.gov/cisa/cybersecurity
[36] https://en.wikipedia.org/wiki/Cyber_threat_hunting
[37] https://en.wikipedia.org/wiki/Emergency_medical_dispatcher
[38] NENA Master Glossary Of 9-1-1 Terminology
https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-ADM-000.22-2018_FINAL_2.pdf
[39] The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final
[40] THE INTERNET OF THINGS: AN OVERVIEW, Understanding the Issues and Challenges of a More Connected World

Land Mobile Radio (LMR) Also called public land mobile radio or private land mobile radio, is a person-to-person voice communication system consisting of two-way radio transceivers (an audio transmitter and receiver in one unit) which can be mobile, installed in vehicles, or portable (walkie-talkies). Public land mobile radio systems are made for use exclusively by public safety organizations such as police, fire, and ambulance services, and other governmental organizations, and use special frequencies reserved for these services.[41]

National Public Safety Telecommunications Council (NPSTC) a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.[42]

Mean Time Between Failures (MTBF) The total time of correct operation in a period divided by the number of failures [43]

Mean Time To Recovery (MTTR) The total hours of downtime caused by system failures divided by the number of failures [44]

Next Generation 9-1-1 (NG9-1-1)A secure, IP-based, open standards system comprised of hardware, software, data, and operational policies and procedures that (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, text, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller; (E) supports data, video, and other communications needs for coordinated incident response and management; and (F) interoperates with services and networks used by first responders to facilitate emergency response.[45]

National Institute of Standards and Technology (NIST) Founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals. Today, NIST measurements support the smallest of technologies to the largest and most complex of

---

https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf

[41] Land mobile radio system https://en.wikipedia.org/wiki/Land_mobile_radio_system

[42] www.npstc.org

[43] MTTR AND MTBF, What are they and what are their differences? https://www.opservices.com/mttr-and-mtbf/

[44] MTTR AND MTBF, What are they and what are their differences? https://www.opservices.com/mttr-and-mtbf/

[45] https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-ADM-000.22-2018_FINAL_2.pdf

human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks.[46]

Originating Service Provider (OSP) An entity that provides telecommunications services to an end user placing a call, or an emergency call or communication (ex., text) seeking emergency assistance.

Platform as a Service (PaaS) The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.[47]

Public Safety Answering Point (PSAP)
An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.

- Primary PSAP: A PSAP to which 9-1-1 calls are routed directly from the 9-1-1 Control Office.
- Secondary PSAP: A PSAP to which 9-1-1 calls are transferred from a Primary PSAP.
- Alternate PSAP: A PSAP designated to receive calls when the primary PSAP is unable to do so.
- Consolidated PSAP: A facility where multiple Public Safety Agencies choose to operate as a single 9-1-1 entity.
- Legacy PSAP: A PSAP that cannot process calls received via i3-defined call interfaces (IPbased calls) and still requires the use of CAMA or ISDN trunk technology for delivery of 9-1-1 emergency calls.
- Serving PSAP: The PSAP to which a call would normally be routed.
- NG9-1-1 PSAP: This term is used to denote a PSAP capable of processing calls and accessing data services as defined in NENA's i3 specification, NENA NENA-STA-010, and referred to therein as an "i3 PSAP".[48]

Software as a Service (SaaS) The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual

[46] https://www.nist.gov/
[47] The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final
[48] NENA Master Glossary Of 9-1-1 Terminology
https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-ADM-000.22-2018_FINAL_2.pdf

application capabilities, with the possible exception of limited user-specific application configuration settings.[49]

Service Level Agreement (SLA) A commitment between a service provider and a client. Aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user. The most common component of SLA is that the services should be provided to the customer as agreed upon in the contract.[50]

Uninterruptible Power Supply (UPS) An electrical apparatus that provides emergency power to a load when the input power source or mains power fails.[51]

[49] The NIST Definition of Cloud Computing https://csrc.nist.gov/publications/detail/sp/800-145/final
[50] https://en.wikipedia.org/wiki/Service-level_agreement
[51] https://en.wikipedia.org/wiki/Uninterruptible_power_supply