GovPilot™

Modernizing Local Government
Information Technology 2023

Comprehensive eBook for IT Officials

2023

The Operating System

for

Local Government

Table of Contents

Summary

Picture this. You're a member of your local government's small and under funded IT department. You just arrived at your office in the morning and checked your email.

Four new emails relating to tech issues arrived from the clerk's department. Three other departments reached out with minor tech bugs. The public works department has been waiting to get their new computer systems installed for weeks and sent another follow up email. Apparently, an administrator just fell for a phishing scam and lost access to critical departmental data. The server in the basement that was installed in the early 2000's needs maintenance. Several departments are waiting on you to help them export data from a spreadsheet so another department can use it.

You'd better get to work on what you can, and need to just accept the fact that some of these things will have to slip through the cracks.

Doesn't this sound like a nightmare? As crazy as this might seem, this is the reality for municipal and county IT departments across the country. A lack of structure and disorganization paired with local governments becoming more reliant on digital infrastructure has created a sea of IT tickets for municipal tech workers to organize and work on.

Follow along to learn more about the problems that arise with a local IT department that is reliant on obsolete systems and processes, and how modern government technology can mitigate these challenges, promote cybersecurity, store public data, help government workers get things done more efficiently, and more.

Unify Departments

All of your data. One platform. Seamless collaboration.

Chapter 1: Forging a Modern Local Government IT Strategy

▍What is Local Government IT?

A local government IT (Information Technology) department installs and maintains computer systems, hardware, and software across a county or municipality. The IT team will primarily handle things like the implementation of cybersecurity protocols, updating antiquated technology across departments, and addressing issues like down wifi, data loss, etc.

When any technological issue arises in one of your governmental departments, the local IT department is the team meant to help you alleviate the problem.

▍Why Is an Efficient Local Government IT Strategy Necessary?

Professional information technology experts are critical for the success of a modern government in order to keep computer systems function and secure. And, as more state, county, and local governments begin to do things like accept permit applications and document requests online, a top notch government IT strategy will be more critical than ever.

▍What Should a County or Municipal IT Department Handle?

A local government IT strategy should include the following:

- **Installing and maintain computer networks**
- **Ensuring cybersecurity protocols**
- **Regularly embracing new technology across government departments**

▍What Are the Benefits of a Great Government Information Technology Strategy?

Your local government will need to embrace government IT software to improve IT department workflows as well as government management software to improve on embracing new tech and cybersecurity.

Here are a few of the countless benefits of the application of modern information technology in government:

1. More Organization in the IT Department with Automated Reporting

Before making the switch to government management software, the Atlantic City, NJ IT department used solely email to receive and respond to tech issues across government departments. On average, it would take over 48 hours to resolve a ticket, with many tickets taking multiple weeks to address.

In switching to GovPilot's IT ticketing software, the IT team received reports of tech issues in one organized and timestamped platform. With automated organization of tickets, the information technology issues could be prioritized, responded to, and completed in just minutes instead of days or weeks. Patrick Quinlan, the Chief Information Officer of Atlantic City was quoted saying, "GovPilot's IT Ticketing module gives us the intel to solve problems that would otherwise take much longer to figure out."

To learn more about AC's transformation to government IT software, explore the Atlantic City IT Department Case Study.

2. Government-Wide Digital Infrastructure

Any good IT strategy is focused on regularly bringing new and innovative technologies into the workplace. To accomplish the goal of having a modern local government IT strategy, you should consider moving to digitized processes across departments.

Here are some of the ways government software can improve every department (and lighten the IT team's workload):

- **Unified Data & Streamlined communications**
  Communicating across departments has never been easier. If your IT department needs to follow up on an inquiry, one government-wide platform allows them to reach out to the relevant department official with just a few clicks. In fact, all government departments can reap the benefit of one simple communication platform.a few clicks. In fact, all government departments can reap the benefit of one simple communication platform.

- **Online applications & document requests**
  Constituents can do things like applying for permits and document requests directly from the government website. Government software integrates these platforms on your government website and stores relevant applications and documents in the cloud. Simple integration means your IT team won't stress about IT issues related to setting up & maintaining online application platforms.

- **Automated scheduling**
  Anything from an IT ticket to a building inspection request will be automatically assigned to a relevant team member via technology known as robotic process automation. That keeps things proactive and holds government employees accountable to get their work done as soon as possible.

3. Proactive IT Posture

With the automated generation and storage of meaningful reports, your IT department will quickly be able to discover patterns in data trends. With clear insights on which types of issues are reoccurring, the IT department can focus on proactively addressing and mitigating tech issues before they become major problems.

4. Cloud-Based Systems = Built-In Cybersecurity

Keeping your government data secure and backed-up is critical for the success of your community and privacy of your constituents. The IT department **must understand cybersecurity best practices and train staff to prevent ransomware attacks and data loss.**

Many modern IT teams are opting to move away from physical storage of government data by turning to cloud-based government management software. The cloud automatically backs-up all relevant government data, meaning your IT and cybersecurity posture is extremely proactive. Additionally, the IT department will save hours of time and significant costs by no longer needing to maintain physical data servers.

GovPilot utilizes the latest Microsoft Cloud technology and automatically backs up customer data every 15 minutes ensuring that data is safe, and accessible no matter the circumstances.

5. 24/7 IT Ticketing

IT software can process, timestamp, and organize IT tickets at any time, day or night. That means that issues can be triaged, prioritized, and solved quickly, efficiently, and with full transparency.

Application of Government IT

Embracing digital infrastructure brings numerous positive benefits for your IT department, budget, and local government as a whole.

In embracing government IT ticketing software, your local government IT workers won't have to stress about organizing, responding to, and fixing issues with obsolete servers or maintain multiple single-use and often obsolete software programs across departments. One seamless platform will keep records, tasks, and submissions organized - ensuring that no tech tasks slip through the cracks.

Implementing government management software across your government departments will improve your budget as updates are pushed directly through the cloud to all users, eliminating the need to maintain a server or conduct costly re-installations of server based software.

An added benefit of modern cloud-based government management software is business continuity. Your staff will be able to login and work from anywhere, on any device, from any location with WIFI. This was essential in the early days of COVID-19 when work from home became the norm overnight. Local governments must be able to operate no matter the circumstance - whether a snowstorm that closes roads, or a devastating flood or hurricane that makes government buildings uninhabitable. A cloud-based solution like GovPilot, gives you the flexibility to serve residents from anywhere at any time.
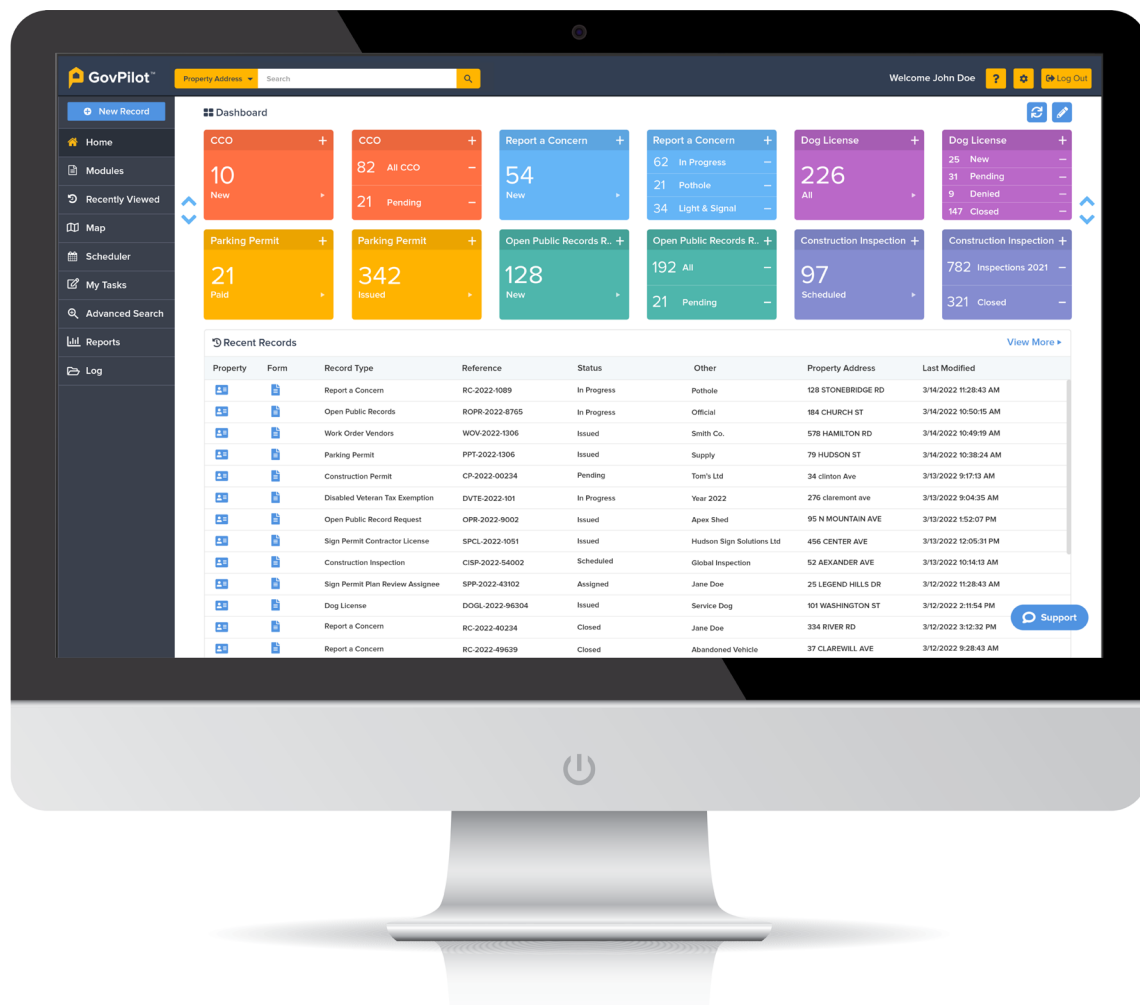
Chapter 2: How to Onboard Government Software

As a government IT official, the idea of bringing digital transformation to your local government is exciting. In addition to unifying cross-departmental data and making your networks more secure, you will be saving your local government and citizens a significant amount of time. Work that used to be done manually in days, will now be able to be done in mere clicks.

With end-to-end digital processes and automated workflows, you'll save countless hours previously spent on mundane manual tasks. Yet, despite all of these proven benefits, there might be a fear in the back of your mind about changing the technological status quo in your county or municipality by making the transition to government software.

What will happen to our thousands (if not hundreds of thousands) of paper records? What will the local government staff that's accustomed to the old way think? Can we afford this? These are reasonable questions most government IT leaders consider when deciding whether or not to go further into the digital realm.

Luckily, making the transition to government software across departments isn't as challenging as it might seem, and the benefits far outweigh the upfront challenges in making the switch to the cloud. With GovPilot, our Onboarding Project Managers will be there to help you every step of the way, and our support staff are available for instant live chats if you ever encounter an issue or have a question.

We've built a platform - with input from real world users - designed to work for local governments of all sizes - from small towns to large counties, and our pricing is accessible for all.

Read on for a full view into the government technology onboarding process.

" **Easy to use and adaptable. It was an easy transition to this (GovPilot) system.** "

Mike Marcum, Code Enforcement
Hermiston, OR

How to Prepare for Onboarding Government Software?

Making the transition to government software is straightforward, especially if you take the proper steps in advance of your onboarding process.

Here are key actions government technology officials can take to work with elected officials and government employees to prepare for onboarding:

1. **Communicate With Your Government Staff**

You may fear that there will be backlash from your government staff for switching processes that have been standard for decades. Yet, even the more hesitant government officials have come to love the benefits of government software when they realize that it handles the most time consuming components of their job and eliminates redundant, manual efforts.

Give the staff a heads up well in advance of your onboarding start date, and be sure to address their questions and reiterate the many benefits to making a digital transformation.

Pro Tip

Communicate with potential new hires about the advantages of your government technology. The best candidates will want to spend their time thinking big and solving problems and will want to work in a digital environment, so letting them know that the most mundane, manual tasks will be automated can be a major advantage in your hiring process. Learn more about Public Sector Recruitment and Key Benefits to Offer Government Workers.

2. Get Paper Records Organized

If your local government is still using paper-based filing, you've likely got thousands of documents filed in various cabinets across departments. If you are looking to adopt GovPilot our team is capable of importing data from previous digital systems or excel spreadsheets. If paper records are critical to carry over to GovPilot they can be attached to digital records once they have been scanned by our new customer or brought over from Laserfiche.

3. Inform the Public

Businesses and citizens alike are accustomed to the status quo for filing applications in-person. Notify them of the upcoming change and timeframe via your government social media, website, and notification channels so that they're fully aware when they will be able to start submitting paperwork and make payments online via modern government IT.

How Does the Onboarding Process Work?

Once you make the decision to embrace government software, there's a standard procedure for getting your local government fully digitized.

Here are the usual steps to move you away from paper filing or on site computer systems into the government cloud:

1. Decide which departments you're going digital in

GovPilot offers 125+ modules for every government department to take advantage of. Choosing an Unlimited plan will allow your IT staff to implement to take advantage of government software in every department for document storage, application submissions, inspections, and other common government workflows.

If you're not ready to make the switch to full digital governance, government leadership will need to decide which government tasks to digitize. You can start with the Essentials (5 modules), Professional (10 modules), or Enterprise (20 modules) plan to see the power of government automation in key government workflows . Keep in mind, you can always scale up once you see the benefits in a few departments!

2. Get existing resources uploaded to the cloud

An Onboarding Project Manager will assist in getting all of your existing digital records uploaded to the cloud for easy access.
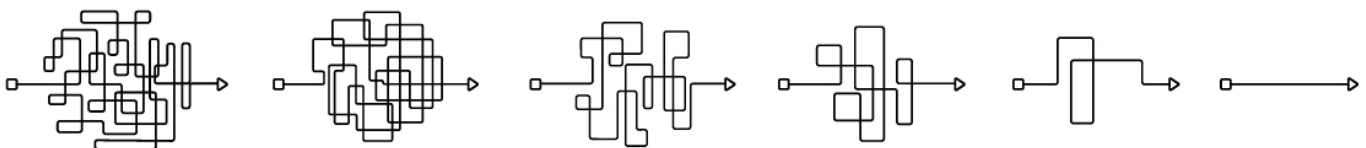
3. Get your staff trained

From day one, your Onboarding Project Managers will work with the government staff to get acclimated to the platform and reap the full benefits of the technology. Government officials have reported feeling comfortable with the technology in just one day, and are typically fully onboarded within 6 weeks or less.

Your government staff will be educated on the cybersecurity best practices to keep your data safe and secure. Learn more about how we Train Local Government Workers on Cybersecurity.

4. Create dashboards and Generate reports

In addition to training your staff, Onboarding Project Managers will work with government leadership to recognize the key KPIs for each department and metrics to track.

Staff can set up tiles in their dashboard to personalize the way records and their status are displayed.

Use sorting functions to organize data sets quickly and easily in order to generate professionally formatted reports in mere seconds. Bring these reports into your next meeting to discuss data, results, and progress.

The IT department can specifically monitor the types of bugs that continuously arise, the amount of time it takes IT officials to address key issues, and more.

5. Keep in touch!

Once onboarding is complete, GovPilot's award-winning Live Support Team and dedicated Account Managers will be on call to assist with whatever questions or needs arise.

Make Your Government Digital Transformation

With the ability to integrate local government software to your county or municipality in just several weeks, the pros far outweigh the cons of embracing government technology. Take the proper steps to educate your staff and citizens, give consideration to the departments you want to move to the cloud, and work with your Onboarding Project Managers to make a smooth transition to automation of your most time consuming responsibilities.

For more details about how GovPilot can transform your government, book a free demo.

Onboarding GovTech FAQs

Is government technology worth it?

Local government technology is straightforward to onboard and offers countless benefits when it comes to saving time by automating manual tasks.

GovPilot customers have reported significant time savings on repetitive tasks, increased productivity, improved local economic development, and money saved. With GovPilot you can do what used to take hours in just a few clicks!

How does government software integration work?

Once you've committed to your government software partner, onboarding specialists will assist in integrating your existing documentation into the platform, training your staff on the platform best practices and cybersecurity protocols, and answering any questions that come up from government leadership or employees.

What types of government software can be onboarded?

GovPilot offers modules to automate processes and move documentation to the cloud across government departments.

Your municipality or county can leverage government technology to:

- Accept online applications for licenses, permits, business registration, document requests, and more

- Perform and record building inspections, health inspections, and more in a simple web based app

- Pull up property records in seconds via GIS mapping technology

- Allow government workers to work from anywhere, at any time (which is a huge selling point for recruiting and retaining government workers)

- Collect fees and fines with credit card processing integrations on your website

What cybersecurity protocols are government officials trained on during onboarding?

The government cloud is often cited as more secure than other forms of data storage like in house servers. That being said, breaches can still occur if government employees are susceptible. GovPilot trains government employees about password best practices, how to avoid phishing scams and other common hacking tactics, and prioritizes two step verification to log into secure government accounts.

Chapter 3: Storing Data in the Government Cloud

In recent years, you've probably heard the term "the cloud" often. Yet, if you're in a local government that still uses paper-based workflows or an in-house computer system for storing government data, you may be missing out on the benefits of being truly cloud-based.

In this guide, you'll get a clear definition of the government cloud as well as information about some of the many benefits it poses for your local government.

What is the Government Cloud?

The Government Cloud is government computer systems that store data over the Internet rather than a physical data server. Data stored in the cloud can be accessed and submitted from anywhere, unlike local servers that require you to be on site to file, store, and access documentation in-person.

For local governments, this poses a serious opportunity to let government officials fill out and access paperwork in the field.

What Are the Benefits of the Government Cloud?

Government officials and staff are constantly out and about. From inspections to emergency management to code enforcement to public works projects, the cloud allows government officials to record, store, and access critical data in the field from a mobile device such as a laptop, tablet, or smartphone.

Here are the benefits in detail that the cloud poses for local governments:in the field.

1. Real Time Data Collection (& Backup)

Government documents will be filed online and automatically stored when you make the switch to the government cloud. You'll have

- Access to records in just a few clicks as soon as they are filed.

- Seamless integration of real-time data into dashboards and reports across departments

- Regular data back-ups to ensure guaranteed access to government data, even in the wake of a ransomware attack or another type of public sector data breach.

2. Cybersecurity

GovPilot has embraced the Microsoft Azure cloud to maximize cybersecurity for local governments. When you embrace the government cloud, onboarding processes include training on the best cybersecurity protocols and how to avoid phishing scams and other notable hacking tactics.

Learn more about Local Government Cybersecurity and How to Train Government Officials on Cybersecurity Best Practices in our guides.

3. Automation of Time-Consuming Tasks

Cloud-based government software is designed to automate mindless tasks across public sector procedures.

- Simple online filing of forms means citizens can submit forms for permits, licenses, etc. without spending hours on the phone or in-person getting help from administrative government officials.

- Documents stored in the cloud are made automatically accessible to all relevant government officials. No more driving to the clerk's office and thumbing through filing cabinets to track down relevant paperwork!

- Tasks like inspections, maintenance, etc. can be automatically assigned from your government software to relevant officials to implement the work.

3. Online Forms

The cloud allows you to make forms - like license and permit applications, business registration, document requests, and more - accessible directly from your local government website. While community members previously had to download, fill out, and a PDF, or file paperwork in-person during office hours, the government cloud allows them to submit digital forms at any time, from anywhere. Automated workflows then notify the relevant public officials upon submission who can then process, approve or deny the request in a remote capacity as well. If the application is denied, officials can send an automatic message instructing the citizen on what they need to do to get approved.

Learn more about How Online Permitting Applications Work.

5. Pull Up Property Records in Seconds

Whenever a permit or license request is submitted, a code violation is issued, an inspection takes place, or any other government interaction occurs at a specific address in your neighborhood, the cloud automatically stores the property records. With intuitive GIS mapping, local government officials can pull up the full set of records for any commercial or residential property in your jurisdiction in a matter of seconds.

Learn more about How to Use GIS Maps in Local Government.

6. Paperless Workflows

Many local governments continue to use paper filing systems that are disorganized, inefficient, and lack regular data backups. This approach results in countless wasted hours spent looking through filing cabinets and boxes for paper records.

Cluttered storage closets and basements, means your government buildings will only get more filled with paper each year. Not to mention the physical danger paper files would be in should a disaster such as a fire, flood, or tornado strike. Once a paper record is lost or destroyed, there is no getting it back.

With a cloud-based government management system, all records, and documents are accessible from a computer or mobile device by all relevant government officials in just a few Harrison Kelly Content Marketing x GovPilot clicks. Save time and eliminate the need to search for records in a filing cabinet. With the cloud your data will be backed up regularly, meaning you'll never have to fear the permanent loss of data due to a storm or data breach. Learn more about the Benefits of Going Paperless in Local Government.

7. Complaint Management

Government officials need to understand the public's perception on how your locality is doing and which issues that matter most to them. Complaint management software allows citizens to file complaints with your local government anytime via a simple mobile app. The complaint is then stored in the cloud, backed up every 15-minutes, and made accessible to the specific department(s) that the issue at hand pertains to. Tasks like infrastructure maintenance will then be scheduled to the public works department and / or other relevant departments, and government officials can message the complainant with any follow-up questions or status updates.

Pro Tip

Encourage constituents to use the GIS mapping feature of your cloud complaint management platform. When a citizen notices an issue like a pothole, flooding, etc. they can drop a pin at the exact location of the issue for your government's reference.

8. Intuitive Government Dashboards & Reports

Local government leadership needs to use concrete data for strategic planning and capital improvement planning. The collection of real-time data and automatic pulling of that data into intuitive dashboards and reports will highlight.

- Government-wide, department-wide, and project specific budgets and where funds are being allocated.

- Revenue being generated by your locality and where it is coming from.

- The types of applications that are being filed by constituents (permits, licenses, business registration, etc.)

- Public approval ratings and the types of issues and complaints that citizens are raising.

How to Transition From Old Data Storage Systems to the Government Cloud?

While this technology may sound complicated for those accustomed to old fashioned data storage methods, making the switch truly is simple. When you go digital, a GovPilot onboarding specialist will come on site to help you

- Transition files from your cabinets or in-house sever into the cloud.

- Educate the full staff on the best practices for using government software in each department and address questions and comments as they arise.

- Provide government employee cyber security training.

Government officials reported feeling comfortable using the technology within just one day, with the full onboarding process typically taking just 6 weeks total.

Beyond onboarding, you'll have more efficient workflows, insightful reports and dashboards, and cybersecurity alongside data back-ups by switching to the cloud. To learn more about GovPilot, book a free demo.

Government Cloud FAQs

What is the Government Cloud?

The government cloud is cybersecure, Internet-based data storage for public sector entities. Unlike disorganized paper-based filing and less secure in-house computer servers, the cloud makes it easy for government officials to remotely access documents online in just a few clicks. Data in the cloud is backed up on a regular basis, to ensure that your sensitive data will always be accessible.

Government Cloud vs Paper Filing: Which is Better for Governments?

Paper-based storage is a disorderly, inefficient, and insecure approach to government data storage. While many governments continue to use this antiquated approach to store documents simply because it's the status quo, these localities are wasting thousands in taxpayer dollars a month in paying officials to sort through various files and cabinets to track down a particular document. And, if something like a fire or flood strikes city hall, your paper records could be lost forever.

Documents are stored and filed online with the cloud, meaning relevant government officials will have automatic access to relevant paperwork and can access it in just a few clicks. Plus, you'll never have to fear the total loss of government documents with regular data backups.

Government Cloud vs In-House Servers: Which is Better for Governments?

Many local governments use on-site servers for managing their computer systems. This system is considered antiquated compared to the government cloud. The cloud makes documents accessible from anywhere, meaning government officials can work from a remote location and / or access paperwork from the cloud. Data stored in on-site servers is only accessible at your place of operations.

Additionally, in-house servers are considered more susceptible to ransomware attacks. While the cloud's regular data-backups will ensure your government data is never lost, data stored in physical servers can be lost permanently by a hack or natural disaster.

Learn more about the benefits in the Cloud vs In-House Servers Guide for Local Government.

What is Microsoft Azure Government Cloud?

GovPilot hosts its platform on the Microsoft Azure cloud. This affords GovPilot and its local government customers with significant benefits including access to the latest Microsoft cloud technology and security which is already trusted by the Department of Defense, the Intelligence community, and 95% of Fortune 500 companies. With local governments increasingly the target of coordinated cyber attacks and malicious ransomware code, Azure is the ideal platform to host local government technology.

With the Azure Cloud, GovPilot and its customers realize significant benefits including:

▪ Enhanced Security: The GovPilot platform is secured with the latest Microsoft technology.

▪ Data Protection: All data is encrypted, and backed-up in multiple locations.

▪ Scalability & Performance: Azure provides limitless room to grow, all while preserving performance.

▪ Business Continuity: GovPilot enables users to access the platform 24/7 from anywhere. Azure allows for rapid restoration of services in the event of natural disaster or other catastrophe.

Chapter 4:
Preventing Data Breaches & Learning From Past Examples

Government data breaches pose one of the largest threats for US government entities and their IT departments in 2023 and beyond. According to the FBI, local governments accounted for the second-highest victimized group in 2021, trailing only the academic sector as ransomware gangs' favorite target.

As geopolitical tensions rise between Russia, Iran, China, and the West, targeted cyber attacks against the federal, state, and local governments are increasingly likely.

But how do you prevent a cyber attack on your municipality? And what happens if a data breach occurs?

Explore this guide for insights into the true costs of a government data breach with real life examples, precautions to take in your locality, and how to immediately respond if a breach occurs in your community.

▍ What is a Government Data Breach?

A government data breach is when private data belonging to a public sector entity is accessed by external forces without authorized permission. Oftentimes, hackers will intentionally trick government workers into unknowingly granting them access to top secret government data. In other instances, unintentional mistakes can lead to private data being made public.

When a data breach occurs due to a hack, the sensitive data is frequently withheld from the government entity unless a hefty ransom is paid. Stolen data can include information about your government affairs, constituents, or private sector partners, meaning it is of the utmost importance to prevent government data breaches from occurring.

▍ Real Life Government Data Breach Examples

Governments of any size are at risk of being hacked. National governments around the world have been hacked, including the United States. State and local governments have experienced major ransomware attacks in which breached data turned into lost data.

Here are some real life examples of government data breaches, and lessons to be learned for your local government:

Government Data Breaches At the Local Level

Local government data breaches are becoming much more common because hackers know that many municipal and county governments are using antiquated information technology systems.

Here are a few examples of local government data loss events that occurred as a result of antiquated cybersecurity protocols:

1. Atlanta, GA's decision not to pay a ransom for stolen government data costs millions in city funds

A 2018 remote ransomware cyber attack against the city of Atlanta's obsolete computer networks left multiple local departments using pen and paper for more than a week. After a remote hacker broke into the system and the city refused to meet the hacker's demand for $51,000 in Bitcoin, the city lost up to $17,000,000 in costs directly related to the hacking event.

Note* - the FBI strongly recommends NOT paying ransom.

The lesson for your local government

Don't wait for a cyber attack to strike to upgrade your local government IT systems. If you're still using physical servers, you're giving hackers an incentive to target your computer systems and exposing yourself to the possibility of losing critical government data forever. Upgrading to the cloud ensures that you're up-to-date with government cybersecurity protocol and have guaranteed data storage back-up of critical data.

Learn more in the guide to Government Data Storage: In-House vs Cloud Servers.

2. 22 townships in Texas Were hit with a coordinated ransomware attack

Even if you're working for a local government in a small township, don't think that means you won't have to worry. Russian hackers targeted small towns across the state of Texas, preventing constituents from paying water bills, the governments from processing payrolls, and government workers from accessing critical government data.

As it turns out, in the middle of the night Texas, Russian hackers across the world "were burrowing into networks," leaving encrypted messages to let local townships know they'd been hacked. The state-wide hack occurred after a private firm connecting Texas communities with a statewide law enforcement database was breached.

The lesson for your local government: Be choosy about private-sector partners you associate with and provide critical constituent data to. When deciding on technology partners, be sure to inquire about their IT protocols and measures to prevent cyber attacks. At GovPilot, we're constantly embracing the latest IT technology meant to prevent cyber attacks including the use of the Microsoft Azure cloud.

3. Fresno, California lost more than $400,000 as a result of a phishing scam

A phishing scam in which a <u>hacker posed as a real contractor</u> working on a public building invoiced the city for $400,000. Changing only the account number and using the contractor's letterhead, a government city employee accepted the payment and sent the hacker taxpayer-funded dollars.

The lesson for your local government

Cybersecurity training for local government workers is critically important for preventing government data breach events. In the situation above, an employee made an honest mistake that could've been avoided with proper training on phishing scams. To learn more about how to train government workers against cyber attacks, read on the <u>Local Government Cybersecurity Training: What to Teach</u> guide.

3. Fresno, California lost more than $400,000 as a result of a phishing scam

A phishing scam in which a hacker posed as a real contractor working on a public building invoiced the city for $400,000. Changing only the account number and using the contractor's letterhead, a government city employee accepted the payment and sent the hacker taxpayer-funded dollars.

The lesson for your local government

Cybersecurity training for local government workers is critically important for preventing government data breach events. In the situation above, an employee made an honest mistake that could've been avoided with proper training on phishing scams. To learn more about how to train government workers against cyber attacks, read on the Local Government Cybersecurity Training: What to Teach guide.

Government Data Breaches At the State Level

1. Texas Comptroller's Office Costs State Millions & Constituents Their Private Data

Government data breaches aren't a new phenomenon. Back in 2011, more than 3,500,000 Texans' names were publicly displayed along with their social security numbers on the Texas comptroller's website for a year until the data breach was caught and addressed.

While Texas law requires that private government files are encrypted, the names and private information were leaked as a result of protocol not being followed. Files submitted from the Teacher Retirement System of Texas, the Texas Workforce Commission, the Employees' Retirement System of Texas, and the Texas Workforce Commission to the comptroller's department were not encrypted, leading to the public display of constituent's most private information.

Millions were spent in notifying constituents that had their information leaked, working with IT consultants to alleviate issues, and in lawsuits with enraged constituents that were affected.

The lesson for your local government

Protocols are in place for a reason. Failure to follow protocol stems from the top, meaning municipal and county leadership needs to keep a keen eye on employees to make sure cyber security measures are being met (unless they want to face harsh criticism from the public when a cyber attack occurs.)

2. Data breach in Georgia's Secretary of State Office exposes 6,100,000 constituents' private data

In 2015, a government data loss event known as the #PeachBreach, left more than 6.1 million Georgian constituents with their personal information exposed,

including , "voter's birthdates, driver's license numbers, and social security numbers.".

The government security breach came as a result of the accidental inclusion of sensitive information in a document regularly distributed by the office to various organizations. Once again, sloppy protocol allowed a lower tier government employee to let the top secret constituent data slip through without internal systems catching the issue.

The lesson for your local government
Documentation being distributed by your local government to the public needs to be reviewed internally as a cyber security measure, even for documents released / updated on a weekly basis. If not, an ordinarily innocuous process could result in personal data of your local government and / or constituents being released to the public.

Government Data Breaches At the National (and International) Level

1. Chinese hackers steal passwords to access to US defense and technology firms

Chinese hackers managed to steal passwords from U.S. firms working with the federal government to steal critical and sensitive information about the inner workings of United States defense technology contracts.

By December, 2021, the number of suspected targets reached 5, with hundreds of other companies posing similar data breach risks at the hand of foreign entities like China and Russia.

The lesson for your local government
Encourage government workers to use convoluted, difficult to guess passwords (like the Google generate a password feature) so that your local government isn't at risk of a data breach as a result of a stolen password.

2. 2022 Cyber Attack on Israel government websites - thought to be the largest in the country's history!

Just days ago in March 2022, the Israeli government faced what may be its largest cyber attack against its government to date. In what's known as a DDos attack, Israeli government websites including the ministry of the defense and ministry of the interior, were inaccessible for multiple hours before being restored.

The lesson for your local government
Russia isn't the only threat you need to be worried about. Threats from geopolitical enemies like Iran and China pose a major threat, and hackers can even be in your own backyard here in the US. In fact, the recent attack mentioned above about Atlanta is speculated to have come at the hands of an Iranian hacker) Be wise about who you're sharing critical data with, especially when

communicating with people outside of your region (and especially if it's international!).

How to Prevent Government Data Breaches?

The honest truth is that cyber attacks will remain an ongoing issue for years to come. As hackers grow more advanced in their techniques, communities that fail to prepare for cyber attacks are preparing to fail.

Here are some ways to mitigate the risk of a local government cyber attack:

1. Spend Federal Grant Funds on Improving Digital Infrastructure

The federal government has approved billions in grants for local governments to improve their digital infrastructure via the American Rescue Plan Act and the Infrastructure Investment and Jobs Act. Both bills grant local governments to allocate funds towards preventing data breaches by improving broadband infrastructure and embracing cloud-based government software.
Learn more with these resources:

- What is the American Rescue Plan? What It Means for Local Government
- Infrastructure Investment and Jobs Act: What It Means for Local Governments

2. Double Down on Your Local Government IT Department

In addition to recruiting great government workers to manage your community's information technology systems, you'll need to have an organized IT ticketing strategy to ensure bugs in the system and / or potential cybersecurity threats don't go unnoticed.

With government management software, IT ticketing is an automated process, where tech issues from other government departments are automatically timestamped and added to the IT ticketing software module for easy accessibility. With GovPilot, municipal workers in Atlantic City reported a decline from 48 hours to respond to a tech issue to just 7 minutes.

3. Avoid Using Physical Servers for Storing Government Data

Physical servers for data storage are obsolete and are prime targets for a cyber attack as a result. Additionally, even if you're not affected by a ransomware attack, a data loss event can still occur if a natural disaster in your community destroys the server. With the cloud, your data is automatically backed up on a regular basis, meaning you'll never have to fear the permanent loss of your government data.

4. Regularly Train Government Workers on Cyber Security Protocols

Phishing scams affect people that are caught off guard every single day. Government workers using '12345' or 'password' as a password gives hackers a chance to break into your local government with just a few guesses. In order to prevent an embarrassing and expensive data breach in your local government, you'll need to offer annual cyber security training that explains **how to prevent data breaches and why this training is growing more important year by year.**

Prevent Local Government Data Breaches

Clearly, whether you're a representative of a major city or a small, local government, data breaches as a result of cyber attacks pose a threat to your community. To prevent the loss of critical data and / or millions of dollars at the hands of a ransomware attack, you'll need to be proactive instead of reactive in adopting secure digital infrastructure. Automate IT ticketing for clear.

Government Data Loss Prevention FAQs

What Are The Best Protocol Measures for Preventing a Government Data Breach?

At a high-level, here's how you should be preventing cyber attacks from striking your local community:

- Offer cybersecurity training
- Use cloud-based software
- Hire qualified IT officials
- Use IT ticketing software
- Ensure private sector partners are using cyber secure networks

How Much Does a Government Data Breach Cost?

A government data breach can cost thousands if you opt to pay a ransom. Recent hackers that stole government data from Atlanta and Newark demanded between $30,000 and $51,000 in Bitcoin for the safe return of government data.

If data is lost for good, it can cost millions to recuperate your losses. After Atlanta decided not to pay their ransom, the speculated cost for the city government was upwards of $17,000,000 in taxpayer dollars.

What Are Common Government Data Breaching Tactics?

A few of the common ways governments are hacked into include:

- Hacking private sector partners to gain access to public sector data
- Phishing scams sent to government workers
- Breaking into antiquated physical servers with easy points of entry for a sophisticated hacker

How to Respond if Your Local Government Data is Breached?

You'll need to work with state and federal officials to overcome a major data breach. Federal departments to contact include your local FBI office, the Secret Service, and the Internet Crime Complaint Center.

In the instance that a hacker demands a ransom for the return of lost government data, you'll need to weigh the pros and cons of meeting (or not meeting) their demands. Not paying the ransom can result in spending millions of taxpayer dollars to alleviate the situation. If you do pay, however, you send a message to other hackers that if they successfully breach your data, they can expect to receive payment.

Chapter 5: Federal IT Grants for Broadband & Cybersecurity

Bead Broadband Grants for Rural Areas

If your government is operating from a rural location, there's a serious chance that you're using far from modern Internet infrastructure. According to the USDA, 22% of rural areas (and 27% of tribal lands) continue to lack modern broadband service.

Without modern Internet quality, your local government can't make a modern digital transformation, is inefficient by current standards, and is discouraging businesses from choosing to operate in your community.

Fortunately, the federal government recognizes the problems with poor broadband infrastructure, and is offering states and territories with rural areas grant dollars to bring modern Internet to their communities.

Follow along for everything you need to know about BEAD grants for rural American townships, and how your municipal or county government can take action to apply funds allocated to your state.

What are Federal BEAD Grants?

As explained by the federal government's Internet for All website, the Broadband, Equity, Access, and Deployment (BEAD) program, "provides $42.45 billion to expand high-speed Internet access by funding planning, infrastructure deployment and adoption programs."

The bill is meant to modernize communities that are falling behind due to lackluster Internet infrastructure. Grants are accessible to state and territory governments and to be applied to rural neighborhoods.

Who is Eligible for BEAD Grants?

The grant, "supports infrastructure deployment, mapping, and adoption," for high-speed Internet in unserved locations (with no access to 25/3 Mbps Internet speeds) and underserved locations (with no access to 100/20 Mbps Internet speeds.)

Applications were to be filed at the state (or territory) level by August 15, 2022. States and territories are expected to work in tandem with local governments to implement the funds in an effective way.
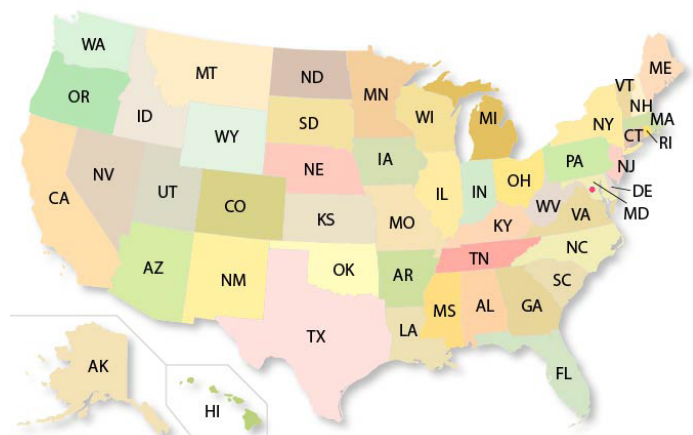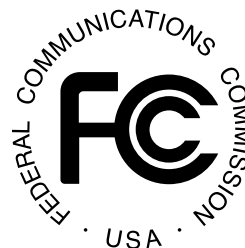
Why is the Federal Government Prioritizing Rural Internet Infrastructure?

Compared to most urban and suburban neighborhoods across the United States, rural Americans tend to have less access to broadband Internet. As most people utilize digital technology and businesses and governments make digital transformations, the Federal government recognizes that rural areas will continue to fall behind as the world and business operations move further into a digital capacity.

Learn more about How Local Governments Benefit From Broadband Internet.

What are the Benefits of Broadband Internet Access for Local Governments?

You might be wondering, why does my rural community even need high-speed Internet? Here are the benefits for your community and local government:

1. Economic Development
Recent Deloitte research highlights that, "higher broadband speeds drive noticeable improvements in job growth." As more businesses move towards digital infrastructure, high-speed Internet can stimulate your community by enticing corporations, entrepreneurs, and remote workers that require high-speed Internet but don't want a big city cost of living.

The bill specifically allows for grants to be used for improving Internet infrastructure in residential multi-family buildings, which can help with increasing local property values.

Here's more tips for Counties & Municipalities to Drive Local Economic Development.

2. Digital Government Workflows
Many municipalities have embraced government software across departments to automate time consuming workflows, collect tangible data, and move business and citizen forms online. Embracing the government cloud is a no brainer for governments using antiquated workflows.

Explore the GovPilot guide about How Automation Can Transform Local Governments for more information.

3. Mobile Government Field Devices
Your local government officials have countless reasons to work from the field, from inspections to code enforcement to infrastructure maintenance. With community-wide high-speed Internet, your government officials no longer need to take notes and file paperwork by hand; they can simply complete all relevant paperwork via a cell phone or tablet in the field and submit it to the cloud. The documentation will automatically be made accessible to all relevant officials across government departments.

How Can Mobile Field Devices Transform Government Field Work? Read on to find out.

4. Improved Government IT Department Functionality
A key component to an effective government IT strategy is maintaining computer systems by modern standards. That means if your locality is still operating with slow Internet and antiquated computer systems, you're doing a disservice to your community. Embracing broadband Internet infrastructure will allow your municipality to upgrade your IT systems with the cloud, automate IT ticketing, and operate a significantly more efficient local government.

5. Online Form Filing

People are too busy to drive to the clerk's department everytime they need to file paperwork. Once your government and citizens have high-speed Internet, point community-members and business owners to your gov-ernment website to file:

- Building and construction permits
- Zoning permits
- Open record requests
- Business registration
- Inspection requests
- Pet licenses
- Government project bids
- Court decision appeals
- ANY other type of form your government frequently uses

Here are more insights into How Going Digital Stream-lines Constituent Services.

6. Online Fee & Fine Processing

If your citizens don't want to drive to the clerk's office to file paperwork, they definitely don't want to do so for paying fees or fines. Luckily, with GovPilot's software in-tegration with various credit card processing platforms, community-members can utilize their new high-speed Internet to make payments online instead of in-person.

Learn more about Modern Government Fee & Fine Pro-cessing.

Can Local Governments File for BEAD Grants?

The Federal government only allowed for states and territories to file for BEAD grants. Your state should have filed by August 15, 2022 to receive funding. That being said, Internet speeds and infrastructure vary drastically from community to community, meaning that your locality can expect to work in tandem with the state to ensure funds are being allocated towards the right projects in your community.

Your government leadership should consider the current speed of your Internet, the types of infrastructure you already have, and the types of infrastructure needed to improve Internet speed for your community and citizens. If you haven't heard from them already, do some research into the department handling Internet infrastructure in your state and consider reaching out to discuss how BEAD grants can be utilized in your community.

How Are BEAD Grant Funds Allowed to Be Allocated?

The BEAD FAQ document outlines the following use cas-es for BEAD grant funds:

1. "Deploying and/or upgrading broadband network fa-cilities in connection with an Unserved Service Project or an Underserved Service Project."

2. Deploying and/or upgrading broadband network facil-ities to provide or improve service to an eligible com-munity anchor institution."

3. "Data collection, broadband mapping, and planning to the extent necessary beyond the planning fund al-location to facilitate the goals and deliverables of the BEAD Program"

4. Installing internet and Wi-Fi infrastructure or providing reduced-cost broadband within a multi-family residen-tial building, with priority given to a residential building that has substantial share of unserved households or is in a location in which the percentage of individuals

household income that is at or below 150 percent of the poverty line applicable to a family of the size involved is higher than the national percentage of such individuals"

5. "Broadband adoption, including programs to provide affordable internet-capable devices"

6. "Training and workforce development." More Internet use means your local government officials need to use cybersecurity best practices. Here is a resource for Training Government Workers About Cybersecurity.

7. "Other uses, including other Digital Equity programs not already included above, proposed by Eligible Entities and approved in advance in writing by the Assistant Secretary that support the goals of the Program"

Bringing Broadband to Rural America

In an increasingly digital world, your local government owes it to your citizens and businesses to have high-speed Internet access. Consider your community's current Internet speeds and infrastructure and work with the relevant state or territory officials to allocate BEAD funds towards bringing modern Internet speeds to your citizens and local government.

Using high-speed Internet will allow your government to go fully digital with cloud-based data storage, online applications, and automated workflows. Learn more about how GovPilot can assist in your digital transformation with a free demo.

Bringing Broadband to Rural America

1. Why Do Rural Communities Need Modern Internet Infrastructure?

The American economy (and global economy in general) is becoming increasingly reliant on Internet infrastructure. For rural economies that already feel as though they've fallen behind, the feelings will worsen if your local government and citizens don't have modern broadband infrastructure for high-speed Internet.

2. How Can Rural Local Governments Benefit From Broadband Internet?

Local governments can move their public records storage and forms to a cloud-based government software platform with proper computer systems. Things like permits, licenses, document requests, and court appeals can all be completed directly from your government website, and government fees and fines can be processed online.

Administrative government tasks can be automated to take things like document filing, scheduling, and document requests off of your government workers' plates with proper government Internet infrastructure and speeds.

3. How Can Rural Community-Members Benefit From Broadband Internet?

Just as your local government will benefit from online forms and payment processing, citizens will be delighted to not have to drive to the clerk's office to file paperwork or pay their taxes.

Most modern businesses tend to function from a digital capacity. Offering high-speed Internet will encourage local economic development as more businesses see the value in operating in your community.

Federal Cybersecurity Grants for Local Governments: Everything to Know

With the passage of the Bipartisan Infrastructure Law, the White House announced, "$1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program," in an effort to put money into the hands of local governments to mitigate against hacks and prevent exposure of sensitive government data as a result of data breaches. But why is the federal government so concerned about local government cybersecurity? And why should local governments feel a need to modernize their computer systems?

Data breaches of local governments are becoming more frequent and costly. Hackers are not discriminating by region either, with cities as large as Atlanta to townships with populations as small as 13,000 in Texas (to even state governments and federal institutions) facing devastating financial consequences and the loss of critical government data in recent years.

Learn more about why the federal government is wisely encouraging local governments to take action, and how you can leverage federal grants to be resilient against ransomware attacks and hackers.

What is the State and Local Cybersecurity Grant Program Program?

President Joe Biden recently announced that $1 billion in funds set forth in the Bipartisan Infrastructure Law is being made available, "over four years to help States and Territories become more resilient to cyber threats."

For local governments, this news means that you're able to start applying for the federal State and Local Cyber Security Grant Program (SLCGP) now as it pertains to upgrading your government information technology systems to prevent ransomware attacks and other damaging cyber attacks.

Why is the Federal Government Taking Action to Ramp Up Municipal and County Cybersecurity?

"Cyberattacks have emerged as one of the most significant threats to our homeland"
- Secretary of Homeland Security Alejandro N. Mayorkas

In recent memory, governments of all sizes and regions have been hacked across the United States. Foreign hackers performing government data breaches are typically in search of critical and private government data, with the goal to collect a ransom for the safe return of the data. When governments refuse to pay the ransom (which the FBI discourages doing) critical data is oftentimes lost permanently. In Atlanta, it cost the city government as much as $17 million in taxpayer dollars to address and overcome a data breach in 2018.

In order to keep your private government data secure as hack attempts against governments continually occur (and often succeed) you'll need to use federal grants and your local government budget to address the issue and improve your IT systems for cybersecurity.

How Can Local Governments Apply for Federal Cybersecurity Grants?

On September 16, 2022, the Department of Homeland Security released a Notice of Fund Opportunity (NOFO) allowing state, local, and territory governments to request grant funds to allocate towards local cybersecurity infrastructure. Within this NOFO, clear instructions are outlined for how a locality can receive grant funds.

At a glance, you'll need to:

1. Coordinate a Cybersecurity Planning Committee.
2. Develop a Cybersecurity Plan outlining what actions you plan to implement with grant funds.
3. Use government key performance indicators to, "conduct assessment and evaluations as the basis for individual projects throughout the life of the program."
4. Implement cybersecurity best practices in your locality.

Here are more details the key actions your municipal, county, or territory government will need to take in order to receive money for local cybersecurity projects.

Coordinating a Cybersecurity Planning Committee

Consider which local government officials within your community are well suited to be on your Cybersecurity Planning Committee (CPC). Consider that your CPC will

- "[develop, implement, and revise a] Cybersecurity Plan"
- work with the chief information officer or chief information security officer (or an equivalent official) to formally approve the Cybersecurity Plan
- prioritize which cybersecurity implementations will be prioritized using grant funds

Cybersecurity Plan

The following data will need to be included in the Cybersecurity Plan formed by your CPC:

- "The eligible entity"
- "Institutions of public education within the eligible [local government's] jurisdiction"
- "Institutions of public health within the eligible [local government's] jurisdiction"
- "representatives from [your] rural, suburban, and high-population [jurisdiction]"

The NOFO specified that your Cybersecurity Plan should be a, "Comprehensive strategic plan to reduce cybersecurity risk and increase capability across the entity...[and] should cover 2 to 3 years." For more details, see appendix two in the NOFO plan.

Cybersecurity Best Practices for Local Governments

Here are the elements laid out as best practices by the Department of Homeland Security that need to be considered by local governments:

1. "Manage, monitor, and track information systems, applications, and user accounts…"
2. "Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts…"
3. "Enhance the preparation, response, and resilience of information systems, applications, and user accounts…"
4. "Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts…"
5. "Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.
   - "These 5 priorities are consider a **must** to include in your Cybersecurity Plan:
     i) "Implement multi-factor authentication
     ii) Implement enhanced logging
     iii) Data encryption for data at rest and in transit
     iv) End use of unsupported/end of life software and hardware that are accessible from the Internet
     v) Prohibit use of known/fixed/default passwords and credentials
     vi) Ensure the ability to reconstitute systems (back ups)
     vii) and Migration to the .gov internet domain."
6. "Promote the delivery of safe, recognizable, and trustworthy online services by the…local governments… including through the use of the .gov internet domain."

7. "Ensure continuity of operations of… local governments… in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident."
8. "Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of…local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel …to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training."
9. "Ensures continuity of communication and data networks within the jurisdiction of the… local governments… in the event of an incident involving those communications or data networks."
10. "Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources…"
11. "Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA."
12. "Leverage cybersecurity services offered by the Department [of Homeland Security]"
13. "Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives."
14. "Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats…"

The DOHS recommends going beyond these elements when applying for federal grants. Consider the Local Government Cybersecurity guide for more inspiration.

How Important is Local Government Technology to Cybersecurity?

If you're using antiquated government digital platforms, or even still using paper and on-site computer systems, you're at serious risk of a data breach. By switching to cloud-based government software, government data across departments will be automatically backed-up and updated in real-time. The cloud is substantially more difficult to hack into than on-site servers, and the regular back-ups ensure you'll never lose access to your critical data. Plus, the onboarding process for GovPilot includes cybersecurity training for local government officials, so community-wide officials will be educated on phishing scams as they embrace digital infrastructure.

As you receive federal grants, your Cybersecurity Planning Committee should consider modern local government technology as an integral part of your Cybersecurity Plan.

Federal Cybersecurity Grants FAQs

What is the State and Local Cybersecurity Grant Program(SLCGP)?

The State and Local Cybersecurity Grant Program (SLCGP) is the allocation of federal funds provided in the Bipartisan Infrastructure Law recently signed into law by President Joe Biden. The federal funds are meant to allow state and local governments to upgrade their cybersecurity measures and protocols as government data breaches become more frequent.

Is GovPilot Cyber Secure?

GovPilot was built to help local governments make a full digital transformation. That's why our digital infrastructure is stored in the cloud with Microsoft Azure. Your local government data will be significantly more cyber secure than using in-house servers (and even more so if your locality used paper-based workflows) and will be automatically backed up to ensure critical data will never succumb to a ransomware attack.

How Can Your Local Government Plan for Federal Grants?

The Department of Homeland Security is requiring local governments to form a Cybersecurity Planning Committee to form a Cybersecurity Plan for your community. To begin, consider the most qualified technology experts in your local government that would be well-suited to set up your short-term and long-term cybersecurity strategy. As your team makes considerations for grant allocation, pay clear attention to the cybersecurity best practices the Department of Homeland Security encourages you to include in your plan, and consider which government technology will best secure your government data across departments.

What Cybersecurity Best Practices Does the Department of Homeland Security Discuss?

Click here for a full list of best practices in Appendix C of the NOFO released by the DOHS.

At a high-level, here are a few local government cybersecurity best practices to consider:

- Your locality needs to have a plan for continuity of government in the wake of a data breach.
- Your IT systems should be moved to the cloud for automated data back-up and better cybersecurity.
- Your local government should have an employee training program in place to educate government officials on the best practices for preventing data attacks.
- Offer digital services from your .gov website with cybersecure government software.
- Instill regular IT check-ups to ensure continued cybersecurity.

Chapter 6: Successful Government IT Ticketing in Practice: Atlantic City, NJ

Explore this helpful case study for insight into how Atlantic City transformed its IT ticketing:

Challenge

With a city workforce of 1,100, Atlantic City relied on a single-use software platform which required employees to send emails alerting IT staff of technology issues or requests. Without a backend management system, IT support requests often took days or weeks to resolve, and many went incomplete, resulting in frustrated employees, malfunctioning equipment and less efficient services for residents.

A key recommendation of the State of New Jersey's 2018 transition report for returning Atlantic City to self-governance, was for the city to invest in software to manage and share data about services and analyze results. The Atlantic City Implementation plan drafted by the state's Department of Community Affairs, detailed that, "such software should result in faster delivery of services provided to residents, greater transparency, faster data sharing between city departments and the public, and greater confidence in city government by residents and the broader community."

Solution

Through a competitive process, officials from The State of New Jersey Department of Community Affairs and Atlantic City thoroughly vetted and ultimately selected GovPilot as the enterprise government management software platform for the city. Atlantic City's Chief Information Officer, Patrick Quinlan worked closely with GovPilot's Customer Success team to deploy multiple modules across several of the city's departments and ensure adoption among employees.

Mr. Quinlan deployed GovPilot's IT Ticketing module across the entire government to streamline the request and response process thereby ensuring that support and procurement are handled in an organized, timely manner.

■ Atlantic City officials previously used a single-use email based software which made tracking, prioritization, and reporting difficult and time consuming.

■ With GovPilot's IT Ticketing software, all requests are time stamped and easily prioritized. Status updates are sent automatically, and report generation is done in just a few clicks.

Results

100% More Efficient

Reporting, response times, and completion rates vastly improved from the previous email-based system.

48 Hours to 7 Minutes

Tickets often took days or weeks to resolve with the legacy system. Now the same issues that once took days, take minutes to resolve.

Proactive Solutions

IT staff are able to identify trends in inbound requests and proactively address problems before they become a major issue.

Available 24/7

IT Ticketing and response are available day and night to ensure essential departments like emergency services remain operational.

" GovPilot's modules makes city government more user-friendly, more convenient and more responsive to its residents. "

Sheila Oliver, Lieutenant Governor of New Jersey

" GovPilot's IT Ticketing module gives us the intel to solve problems that would otherwise take much longer to figure out. "

Patrick Quinlan, Chief Information Officer

GovPilot™

The Operating System for Local Government

Web	http://govpilot.com
Email	sales@govpilot.com
Phone	800.491.6732

GovPilot - named a GovTech 100 company for six consecutive years - is the leader in digital transformation for local governments. GovPilot's cloud-based platform was built with the sole purpose of enabling local governments to operate at their full potential by standardizing, digitizing, and unifying more than 100 operational and constituent service processes on one system.

To learn more visit www.govpilot.com. Follow @GovPilot on LinkedIn and Twitter.