**Testimony of Keisha Lance Bottoms**
**Mayor, City of Atlanta, Georgia**

**Subcommittee on Cybersecurity, Infrastructure Protection and Innovation**

# Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help

**June 25, 2019**

Good afternoon. My name is Keisha Lance Bottoms and I am the Mayor of Atlanta, Georgia, the cradle of the Civil Rights Movement and the anchor of the 10th largest economy in the United States.

I want to thank Chairman Bennie Thompson and Subcommittee Chairman Cedric Richmond for inviting me today to testify at this important hearing. I am honored to be here.

In the early morning hours of Thursday, March 22, 2018 – 77 days after I was sworn in as the 60th Mayor of Atlanta – the City experienced a ransomware cyberattack which impacted our operations and our ability to provide services to our residents and visitors.

Fortunately, mission-critical services such as fire, police and ambulance services, and our water supply, were not affected.

However, some departments and governmental entities suffered irreparable damage.

The Atlanta Municipal Court had to cancel and reschedule hearings, suffering a major interruption. ATL311, our customer service interface for our residents, was knocked offline.

Many other applications were impacted or affected, delaying the provision of services by the City.

As that first day unfolded and the City learned more details about the disruption, it became clear to us that criminals had attacked the City's systems.

As this Committee knows, one of the most common and successful ways that criminals can attack entities is through phishing. Phishing scams use social engineering to trick a user into clicking on a link which can then infect the system with malware. Depending on the malware used, it can take over and encrypt the user's computer. Ransomware can also delete or permanently corrupt files and destroy them forever, something we experienced in Atlanta.

The City of Atlanta moved quickly to address the impacts and to mitigate the attack, notifying law enforcement and key partners, including our insurance carrier, outside counsel, government partners and the media. We also hired an outside cybersecurity firm to assist with our response.

While like other crimes, in the case of a cybersecurity attacks, it can take days and even months to fully understand the depth and breadth of what may have been impacted.

The City assessed which systems, functions and operations were impacted. That might sound simple, but during an emergency, identifying every compromised system was difficult to accomplish, especially without the assistance of technology.

Although the overall impact was not substantial throughout our infrastructure, we took some systems off-line out of an abundance of caution.

The City soon learned that the attackers were demanding a ransom payment of $51,000 in Bitcoin to unlock our systems, which we refused to pay.

The cost of recovery to date has been about $7.2 million and we expect it will go higher.

Some costs have been reimbursed under Atlanta's cyber-insurance policies, with the hope that more will be reimbursed.

However, cyber insurance policies vary greatly, and not all policies cover the wide-ranging impacts that a cyberattack can do to a company or a city. It is critical to seek expert advice and counsel to ensure that the policies purchased can cover the damages that can be sustained.

As this Committee knows, in November 2018, the U.S. Department of Justice charged two Iranians with the attack and outlined the wide-ranging plan they crafted to attack countless local governments, health care systems and other public entities.

Unfortunately, the City of Atlanta's cyberattack was not an isolated occurrence. As organizations integrate technology into every aspect of our lives, cybersecurity risk is ever present. If not secured, systems across public and private entities will continually be subject to attack and digital extortion.

Cities such as Savannah, Georgia; Dallas, Texas; and Baltimore, Maryland have been attacked. The attack in Baltimore affected its 911 system, which further underscores how these attacks threaten the actual health and safety for each of us.

Cyber threats are becoming more hostile and frequent, so all organizations must understand how to protect themselves against these attacks when they do occur.

The good news is that the City of Atlanta is using its experience to become a "model city" for how municipalities can protect against, and prepare for, cyberattacks.

We are adopting a more flexible and hardened infrastructure by utilizing advanced technologies in order to diversify and minimize risk.

We are emphasizing the importance of cross-functional incident response teams that include federal and state government partners.

We are strengthening our human capital to make certain that the best and the brightest are guarding our systems.

We are in a good place going forward. Atlanta and the State of Georgia represent one of the nation's elite cybersecurity hubs, ranking third in the nation with companies that focus on information security, and generating more than $4.7 billion in annual revenue.

More than 115 cybersecurity firms call Georgia home, including Cybersecurity 500-ranked Secureworks, Pindrop, NexDefense and Ionic Security.

Based on the City's "lessons learned" we can now help other cities to take cybersecurity seriously and plan to put in place manual processes for mission critical applications and services to specifically address cyber risks

This includes ensuring cities have carried out a thorough risk assessment of their systems, including both infrastructure and business practices.

No city can do this effectively without partnerships. The City of Atlanta has worked with the FBI, the Department of Homeland Security, the Secret Service and the private sector. The work done to prepare for Super Bowl LIII (53) was a great example of these collaborative efforts.

The priority at the City of Atlanta is to build a culture of cybersecurity where all our technology experts and partners are around the table.

We intend to stay pro-active in order to understand and manage the ever-evolving landscape.

We are re-focusing on operational basics- Detection, Response and Recovery.

On detection, we need to be able to quickly identify anomalies and potential issues;

On response, once a problem is identified, we need to rapidly seek to contain the risk;

And on recovery, we will better understand the impacts of an attack and have cyber specific recovery and business-continuity plans in place ready to be deployed immediately.

One component of a "down to the basics" plan is to have an ongoing program to educate employees and help them identify a phishing email; as well as require the use of strong passwords, and prioritize funding and empower cyber leadership, as we have done in Atlanta.

Regardless of the protective measures that are employed, cybersecurity risks are now part of our everyday lives. We've learned that you can never completely protect a computer network.

But there are steps that can be taken.

For example, cities should establish clear processes and be ready to implement their cyber incident-response plan, just as they do in anticipation of other emergencies.

While the City of Atlanta is more prepared and more resilient, many local and state governments are not, and need the help of the federal government.

Specifically, the federal government can help by passing legislation and providing funding to assist state and local governments in preventing, preparing for and responding to cyber threats and incidents. It is also important to emphasize the need for the federal government to provide emergency funding and support during an actual cyberattack. Having access to funds at the time of an attack would not only accelerate responsiveness and restoration; but, would also result in fewer municipalities paying ransoms and ultimately decrease the occurrence of local governments as targets.

Second, the federal government can assist by empowering its agencies to develop and share best practices with state and local governments. Many small municipalities do not have the resources necessary to development and implement these best practices.

Third, the federal government should expand its programs that share real-time threat information with state and local governments as this information is often critical in avoiding or mitigating threats.

Next, when an attack does occur, the federal government should have programs in place to provide cybersecurity disaster relief funding to help offset recovery and restoration costs borne by state and local governments.

Lastly, many state and local governments administer elections and need help in ensuring the safety and security of the electoral process.

We are living in a different digital world now. Nation-state actors and other foreign adversaries are attacking our state and local governments and we need a strong federal partner to defend against those threats.

We know the threats will continue. What we're planning for today may look different tomorrow.

With the support and assistance of partners such as the U.S. Department of Homeland Security and this distinguished Committee, all our cities, and our country, can be safer by being prepared.

Thank you.