SUTHERLAND
GOVERNMENT SOLUTIONS

*Processes & Solutions for Smart Government™*

# Protecting and Analyzing Data; Trends and Holistic Approaches for State and Local Governments

## Securing Sensitive Data: Threats and Proactive Responses:

Securing sensitive data is a top priority for government and industry. In recent years there have been more than 200,000 cyber incidents annually involving government agencies, critical infrastructure and industry partners. These incidents are not sector-specific and represent a challenge to preparation, budget and technical resources.

An evolving threat called Ransomware, largely delivered from Phishing attacks, have become one of the preferred means of hackers targeting agencies and companies. Last year, FBI reported more than 2,500 incidents of ransomware. The figures are likely much higher as most companies and organizations do not want to publicly disclose that they have been breached, and especially extorted. Ransomware is a growing state and local problem.

As a result of breaches and more sophisticated threats, the trend in government and industry appears to be changing from reacting to being more proactive. The newer approach is for a more holistic approach of integrating technologies, processes and people. The future of the practice will rely more on informed risk management. That requires an active strategy of detection, recognition, identification, response and remediation of threats. Advancement in area of predictive data analytics and diagnostics to index, provide network traffic analysis, and protect against further incursions is already becoming a growing area of concentration.

Technology development continues to evolve with the introduction of new innovations to address the cybersecurity framework that includes networks, payloads, endpoints, firewalls, anti-virus software, and encryption. This framework will provide for better resiliency and also forensic analysis capabilities. Some newer areas of cybersecurity spending will be in the areas of cloud, authentication, biometrics, mobility, automation, including self-encrypting drives. And, of course, super-computing and quantum computing. Automation, including via artificial intelligence, is an emerging and future cybersecurity pathway. This model has the potential to be expanded and upgraded both in the public and private sector.

## The State and Local "Cybersecurity Tool Chest": Capabilities and Services Needed to Secure State & Local Governments

There are a variety of capabilities and services in information assurance and cybersecurity required to ensure the protection and analysis of data in State & Local governing. These can include:

- Compliance and compliance training
- Penetration and vulnerability testing
- Mitigation response: service of informing and servicing victims of breaches
- "Real-time" horizon scanning and monitoring of networks
- Document integrity and authentication
- Identity management
- Analytics capabilities for informed risk management
- Social media threat analytics
- HR managed services for expansion of hiring and training of the emerging cybersecurity workforce
- Waste, fraud & abuse
- Risk management consulting and trusted cybersecurity advisory
- Subject matter expert (SME) staff augmentation

## Cybersecurity in Elections:

Elections are first and foremost about securing databases. States and County localities manage elections that include a variety of types of election machines, databases, and processes. It is a primary role of state officials to ensure that the integrity of elections are not disrupted by breaches, cyber of physical.

The NASS official document on Cybersecurity and Elections states: As our federal intelligence agencies have repeatedly **emphasized**, state and local autonomy over elections is our greatest asset against malicious attacks and systemic fraud or rigging. There is no way to disrupt the voting process in any large-scale, meaningful way through cyberattacks because there is NO NATIONAL SYSTEM to target and state election systems do not have a lot of Internet connectivity. As a result, officials at all levels of government have affirmed the **structural integrity of our electoral process**.

### 5 Elements of Election Cybersecurity:

The best approach to ensuring election integrity is for states not to abandon autonomy but to upgrade and reinforce capabilities from the existing "Cybersecurity Tool Chest." Specifically, a state and local cybersecurity election plan should include: 1) incorporating risk management assessments of the vulnerability of machines and sensitive data bases; 2) enacting a program of encryption and cyber hygiene to guard against phishing attacks and insider intrusions; 3) monitoring of the networks and data bases; 4) identity and document authentication and management; 5) mitigation response – or redundancy and resiliency if systems are compromised. Effective election cybersecurity also includes cooperation with the private sector.

## Cybersecurity: The Importance of Public/Private Cooperation at the State and Local levels

Keeping up with cybersecurity threats is often daunting and requires a holistic effort. There are a wide variety of architectures, systems, and jurisdictions and adaptability and scalability to upgrade to new security technologies and processes is a significant challenge.

Whether it be elections services, business services or securing operational databases, a broad-based cybersecurity strategy for securing government, must include investing in next-generation tools and workforce, and empowering citizens.

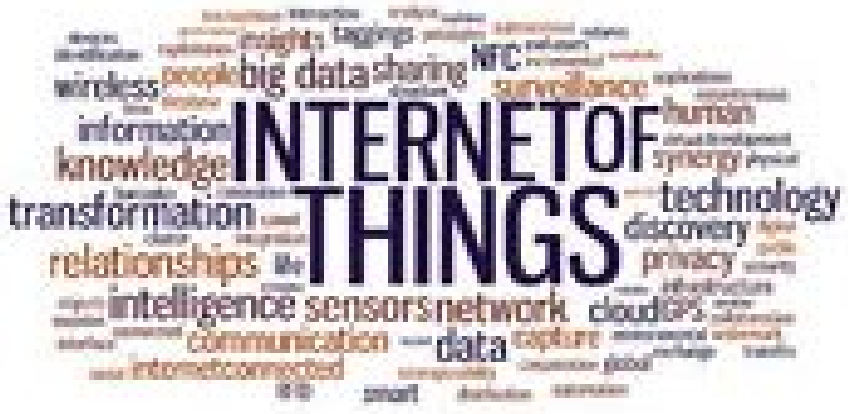
While there is an array of promising technologies being developed, there are is no immediate technological panacea to stop intrusion. But there are promising technologies that include better encryption, biometrics, smarter analytics, automated network security. Informed risk management planning, training, network monitoring, and incorporating Next Gen layered hardware/software technologies for the enterprise network, payload, and endpoint security. All of these are all components of what can be improved via cooperative efforts in research, development, and deployment efforts.

A closer partnership between state and local governments and the private sector could help produce tactical and long-term strategic cybersecurity solutions quicker. Cooperative research and development in new technologies such as hardware, software algorithms and operational processes are needed just to keep up with the evolving global threat matrix. There are no areas on the cybersecurity spectrum that do not need more investment and modernization to help fill capability gaps.

A critical element of public/private partnering also includes information sharing between the Public/Private sectors. In a rapidly changing threat landscape it is important to be able to provide situational awareness and coordinate protection, prevention, mitigation, and recovery from cyber incidents. In state government, the threat landscape includes threats to utilities, hospitals, law enforcement, transportation, and private databases.

To incorporate true cybersecurity protection, it call comes down to a basic security awareness of employees, establishing security protocols, and having a trained work force. A wide variety of technologies, protocols, SMEs working in a holistic approach will be fundamental to the success of cybersecurity at the state and local levels. This should be inclusive in any framework and cooperative strategy as we move ahead into a new digital era that includes the emergence of the Internet of Things.

## New Challenges for State and Local Governments-- The Internet of Things (IoT)




The Internet of Things (IoT) is the concept of connecting any device to the internet, from home appliances to wearable technology such as watches, to cars. These days, if a device can be turned on, it most likely can be connected to the internet. Because of the IoT, objects to objects, people to people and objects to people can communicate quickly and efficiently.

As we enter into a digital era comprised of billions of connected devices, smart cities, smart homes, smart businesses, and smart governments - almost everything and anything will be interfaced with sensors and fully automated in the near future. The role of securing these

devices and sensors becomes paramount.  It's safe to say that our lives are going to be transformed completely because of digital technology.

According to the McKinsey Global Institute, the Internet of Things (IoT) has the potential to impact economies up to $6.2 trillion annually by the year 2025. Just like many industries, government agencies are looking for ways to cut costs and become more efficient, and have realized the IoT is one way they can achieve productivity gains. Over the last five years, the federal government has spent more than $300 million on IoT-related research and Cisco estimates that the IoT will be valued at $4.6 trillion for the public sector in the next ten years.

In the public sector, government agencies are being tasked to keep pace with expanding customers service requirements emanating from the connected economy. New citizen engagement strategies involving technology, policy, programs, and intra/inter-agency collaboration are required to address the avalanche of needs and fixes associated with interoperability and cybersecurity of the IoT of smart government.

**Sutherland Government Solutions (SGSI)** is a part of Sutherland Global Services (SGS) and its mission is to ensure governments will meet their vision of fully responding to citizen mandates. As a trusted solutions partner, SGSI delivers smart, affordable and highly responsive processes and solutions to deliver "integrated services" – to enhance the customer experience and deliver results. SGSI has deep expertise in IT Services and system integration, is agile and is able to rapidly deploy to meet government requirements, and has relevant and strong commercial platforms and experience that is critical for success in the cybersecurity space.