Statement on Senate Substitute for HOUSE BILL NO. 2331: Supporting Citizens in the Digital Age: Leading Practices

March 13, 2017

Hon. Mark Forman
Global Head, VP and General Manager, Public Sector
Unisys Corporation
Previously First U.S. Administrator for E-Government and IT

Dave Leichner
VP Public Sector - US and Canada
Unisys Corporation

Summary: Unisys-commissioned research documents a rapid shift in citizen desires and expectations for interacting with government in the Digital age. For example, our most recent survey of citizens in five countries show two-thirds of citizens want to engage government online or by mobile apps, more than double the number one year ago. Coupled with results from our recent Safe Cities and Security Index global surveys, our research shows citizens want government to improve cybersecurity, consolidate redundant data collections and systems, and make use of digital technologies to simplify interactions with citizens. Today's leading state governments combine citizen service improvements with IT modernization initiatives to lower cost of operations, improve responsiveness to citizen needs, and reduce cyber security risks. To accomplish these gains, a new IT operations model is rapidly spreading across state and federal governments, with the core components being shared services and cloud computing.

Mr. Chairman and members of the Committee, thank you for allowing us to provide neutral comments on the legislation before the Committee today, Senate Substitute for HOUSE BILL NO. 2331. My purpose in testifying today is to provide the Committee with insights on leading government IT practices.

Citizens Expect Their Government to Move into the Digital Age

In order to inform government decision makers and improve the quality of our work, Unisys conducts surveys and focus groups on the changing needs and challenges of the digital age. Unisys's **2016 survey of U.S. Federal and State C-level executives**[1] found strong belief in digital government approaches to improve speed and quality of service delivery. It also identified key constraints including cyber security risks, availability of knowledgeable staff, time and cost of initiatives, and organization change management. Last year, the **Unisys Security Index**[2], found that 68 percent of Americans are highly concerned about cyber and physical security – up by nearly half in the past two years. During the last two months, we released two survey reports, **Safe Cities: Where Smart Becomes Safe**[3] and **Connected Government: Insights Into Improving Citizen Services**[4]. The Safe Cities report highlighted the need for law enforcement agencies to embrace a two-way street in the use of digital technologies, such as social media, where police obtain key information and insights as well inform the public using apps such as

[1] www.unisys.com/digital-government
[2] www.unisys.com/unisys-security-index
[3] www.unisys.com/safecities
[4] www.unisys.com/digital-government-apac

Twitter, Facebook, and WhatsApp. The Connected Government survey report found that 63% of citizens now want to use smart phones and computers to interact with government, more than doubling last year's 31% result. In addition, the report highlighted that citizens want to access services through a single mobile app or portal, rather than having to use a different website or app for different government agencies and programs. These surveys found key citizen concerns on cybersecurity and trust in government, including:

- Nearly two-thirds of the public would report a crime (63%) or upload evidence on a crime that had just taken place (63%), but 40% of the respondents were worried that their messages would not reach the right person or that the government's technology might fail.

- The overall Unisys Security Index for the U.S is 169, which is considered a serious level of concern, up from 123 – which was considered a moderate level of concern – in 2014. This marks a 37 percent increase in Americans' overall security concerns since the last survey.

- Nine out of 10 citizens assume that government agencies are already sharing personal data, especially basic information such as demographics, tax file numbers or identification codes.

- 63% of people strongly believe "It should be a lot easier for people to contact the police through digital media in this day and age." People believe it would enable faster reporting of crimes and make it easier for witnesses and victims to provide key information, such as videos, to police. But only 33% of US citizens believe that federal, state, and/or municipal government is extremely trustworthy "when it comes to using technology to prevent and investigate crimes."

Over that last year, Unisys also conducted **focus group "listening sessions" with government CIOs**, who identified four key areas of focus: Remove Costs; Increase Security; Create a Consumer-like Citizen Experience; and Use Open Data to Create Transparency, Insights and Visibility into services, performance, and operations.

Challenges and Constraints

In order to provide a more digitized and citizen-customer centric model, government must modernize many of its IT systems. Five constraints impact success:

1. **Challenges with IT Lifecycle Management.** States are often balancing a patchwork of funded and unfunded initiatives that cut across multiple generations of technologies. As a result, government systems are outdated, in some cases behind as much as fifty years. Governments must address ongoing operational needs, such as patching software vulnerabilities for multiple generations of technology, while trying to successfully integrate new solutions to better meet citizen needs. Demands do not end when new technologies are purchased, governments must keep both the new and legacy technologies performing as expected and secure. The mix of modern and legacy technologies often coupled with outdated IT management practices often lead to excessive IT expenditures because of inaccurate inventory data and difficulty determining what systems are no longer needed.

2. **Skills Development and Acquisition.** It is difficult to maintain government-employed talent with large percentages of the workforce eligible for retirement. Due to government IT compensation levels, the ability to acquire and retain quality talent is a challenge: in some states we see attrition of 25% while the industry average is at 10%. Thus, we often see insufficient qualified numbers of in-house staffing needed to acquire new technologies and manage the IT environment.

3. **Historically Siloed Systems Bring Multiple Challenges.** Historically, every new regulation or government program created its own information system, generally involving a form that was filled-

out and stored in custom-built data base. As a result, Information Technology is either managed by many government departments or by an improvised contractor ecosystem which does not easily adapt to changes in laws and citizen needs. The result is that each new law generates a new system in an increasingly complicated patchwork spaghetti of systems, which are expensive to maintain and hard to secure.

As a result, State data centers often experience the following common challenges:

- Systems, networks, and facilities in need of significant repairs
- Lack access to funds to address key IT systems security and operations needs
- Lack service level agreements and line of sight to costs and actions for achieving performance
- Lack standardization in operating, management, and reporting techniques needed to improve efficiency and achieve economies of scale

4. **Inability to Gain Data Insight**: Due to the siloed systems, data is stored in different formats and languages, generally focused on documents and approval workflows. In most cases, systems cannot interoperate or communicate between one another, creating silos of information that limit the collaboration and information sharing needed to address today's policy needs, such as the opioid crisis. As a result, governments are unable to obtain insight from the vast amount of data stored in these systems.

5. **Large scale "rip and replace" projects fail 75% of the time:** Complexity, size, and highly customized nature of government systems result in expanded costs, reduced functionality, and late delivery of large scale system modernization projects. Governments need a structure that pairs incremental system transformation with immediate citizen benefit.

Overall, most state governments have several generations of systems operating that are costly to maintain, difficult to keep operating, and hard to secure. State governments need a governance approach to IT that can better manage costs, support agency needs, and reduce cybersecurity risk. Even more, state governments need to be able to mesh *analog* forms-based systems with *digital* approaches that use data and algorithms to better address today citizen needs.

Solution: Acquiring IT as a Service

Maintaining a modern government requires access to skilled staff and modern technology. State governments have a simple choice: Make large investments in new people and new technology, or take advantage of cloud computing and acquire IT as a Service.

The quality, security, and cost of Information Technology is defined by how well an entity can take advantage of economies of scale. Although it is hard to overcome parochial desires for each agency or program to "own" a customized system, the siloed approach to IT is no longer viable. Over the past 10 years, the shear economics have driven the IT Industry to shift to cloud computing, a model where IT systems are chunked up and converted to services that take advantage of economies of scale in security, computing power, storage, and plant and equipment. Governments are now making the change, with Digital Government spending now at 17% compound annual growth rate, compared with 5% growth in overall government IT spending, according to our market research.

There are two components to make the transition. First, there has to be a governance model that oversees the shift to a shared services approach. Generally, states couple an Executive Branch IT governance regulation with a law that provides clear guidance on authorities, accountabilities, and follow-up review. In the leading practice, current siloed systems are transitioned to a shared services environment for operating infrastructure and business applications, using a hybrid private/public cloud. A benchmark example would be the State of New York's SAGE report, which created clusters of agency systems to facilitate better insights and collaboration for improved mission results (e.g. Social Services). Another example would be the State of New South Wales, Australia, which created parallel citizen services transformation (ServiceNSW) and IT shared services (GovConnect). ServiceNSW identifies citizen-centric transformation initiatives and GovConnect provides the IT to support the initiative.

Second, governments are adopting an acquisition strategy that overcomes today's challenges and facilitates the shift to IT as a Service. States undertake a competition to identify a best value vendor partner that can be held accountable for operations, maintenance, and innovation of the IT environment. Implementing this acquisition strategy can remove capital investments from the books of government. In this model, government pays only for the amount of IT consumed. Government oversight shifts from inputs, such as the cost of hardware, to performance results of the vendor partners. Leading governments use a performance-based contracting approach where the government receives acceptable level of performance via service level attainment (SLA), or the vendor partner is penalized financially.

To be successful, acquisition and governance strategies need to include Customer Relationship Management (CRM) to define and deliver the benefits for participating agencies that take advantage of the shared services approach. The most difficult element in change is not the technology but addressing the human need—people's willingness to change when presented with a better deal. As part of that willingness, strategies need to include clear communication of benefits to agencies and to the individuals who deliver services. This requires a focus on business requirements as well as technical requirements. CRM is critically important to increase successful adoption of new services.

The result of implementing this shared service model enables the government to unlock the power of effective IT management in several areas:

1. Savings can be created by single point of negotiation with vendors. This approach provides transparency into costs relative to consumption so all departments receive equally beneficial value. No one agency bears a larger share of costs than its level of IT usage would require.

2. Individual talent can be focused on government's mission and business needs, given the assurance that technology and services are delivered and measured on a performance contract with the external vendor partner.

3. Costs of service, including unused IT, are made visibile so that savings can be identified and used to reinvest in needed initiatives.

4. Data from siloed enivornments can be harvested to gain insight into how to better serve citizens, predict and scale for future needs, and achieve performance transparency across the government

5. Potential areas of service impact can be addressed proactively so citizen service is never interrupted

6. Citizen-Customer usability concerns, like having to go to multiple websites for services, can be addressed

Further, when security governance is coupled as a requirement to this acquisition approach, the vendor partner is accountable for supporting not only managed security services but regulatory requirements like the Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and Information Security Risk Management for Canada (ITSG-33).

Benefits: Examples from Government Deployment

While there is no comprehensive study of documented benefits, we have some representative examples:

> **Large Northeastern US State** applied the shared services model to modernize social service program delivery and reduce costs. In their pilot project, a multi-million dollar investment achieved a 500% rate of return in cost savings while delivering better services to citizens.
>
> **Large State in Australia** applied the shared services model using a hybrid cloud. In the initial phase of deployment they reduced operating costs by more than $10M per year through retirement of applications that became visible as no longer being used.

Conclusion

The insight we received from commissioned research and Unisys-Leader conversations confirms improvements in IT governance and the shift to IT as a Service enable the change needed to address today’s multi-faceted policy issues and support the new digital world of the customer-citizen.

Supporting Citizens in the Digital Age: Leading Practices

Hon. Mark Forman
Global Head, VP and General Manager, Public Sector
Unisys Corporation

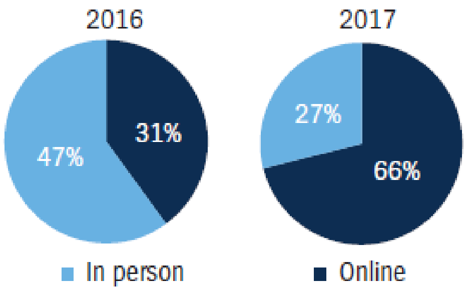
Dave Leichner
VP Public Sector - US and Canada
Unisys Corporation

March 13, 2018

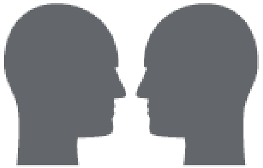
Citizen Expectations in a Digital Age

Unisys Connected Government Survey of 5000+ citizens in Australia, New Zealand, Malaysia, the Philippines and Singapore provides insights into how people prefer to engage with government and if they support government agencies sharing citizen data with each other

Preference to use online channels is growing



Face to face still preferred for 2-way interactions



- renewing a driver's licence or passport
- applying for benefit payments
- obtaining building permits

People want a single point of contact

63% of all citizens surveyed prefer a single app with access to multiple government agencies

Five Requirements for Effective Digital Transformation

A complete journey: Agencies should provide citizens with the ability to start a transaction online and then complete it via another channel.

Online and offline: Look at innovative ways of making services accessible to as many as people as possible, including those without access to a device or the internet.

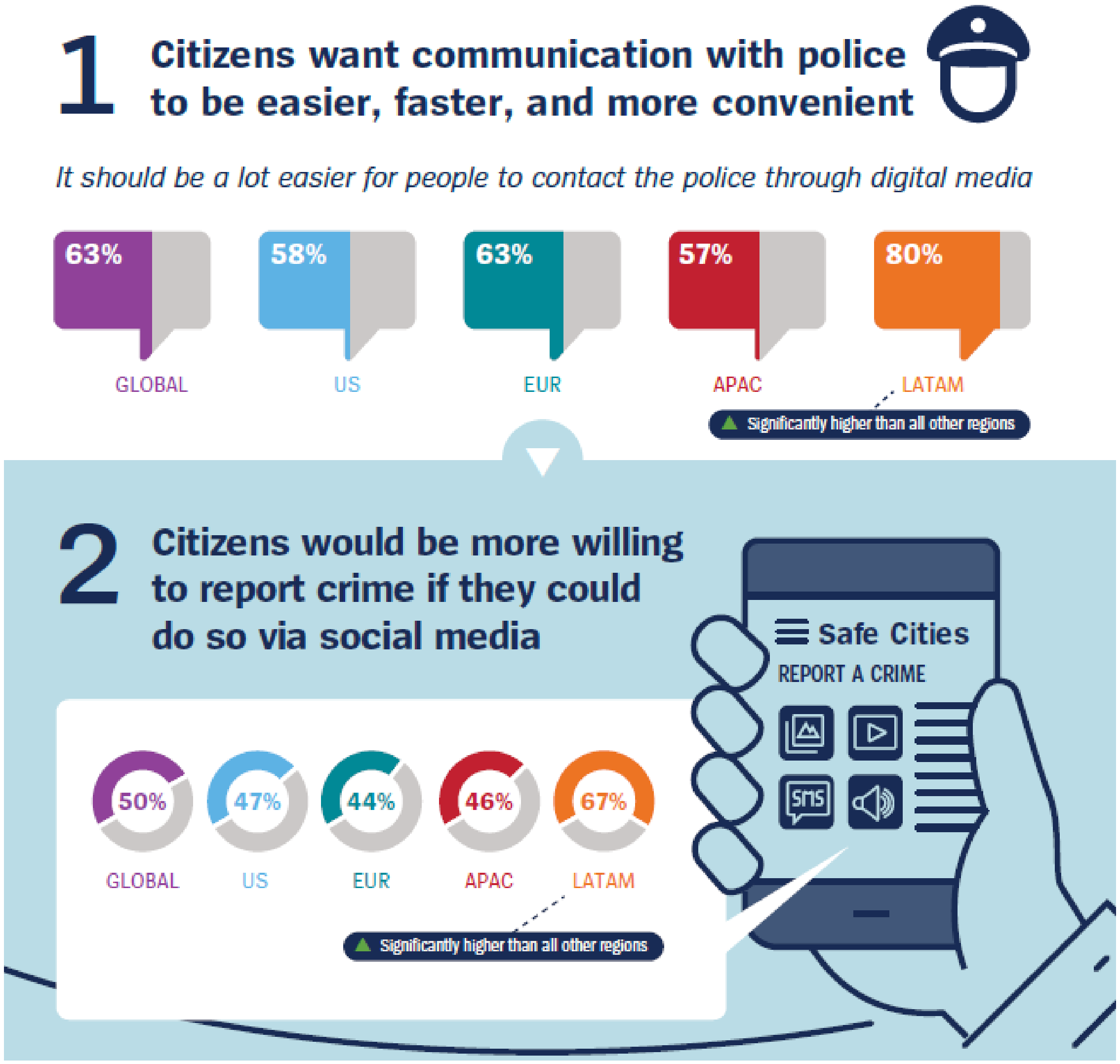
Team effort equals better outcome: Bring teams together to collaborate and adopt an agile approach that can be used to design, trial, test, adapt and evolve new concepts and ideas with citizens early in the development process.

Joined up services: Agencies should look for opportunities to deliver joined up services where citizens can access multiple agency services through a single website or app.

Engagement: Engage with citizens in a two-way street, such as making digital services accessible via interactions in social media platforms such as Facebook, which are the go-to apps for millennials.

Visit: www.unisys.com/digital-government-apac

Safe Cities Survey – 2017 Global Study

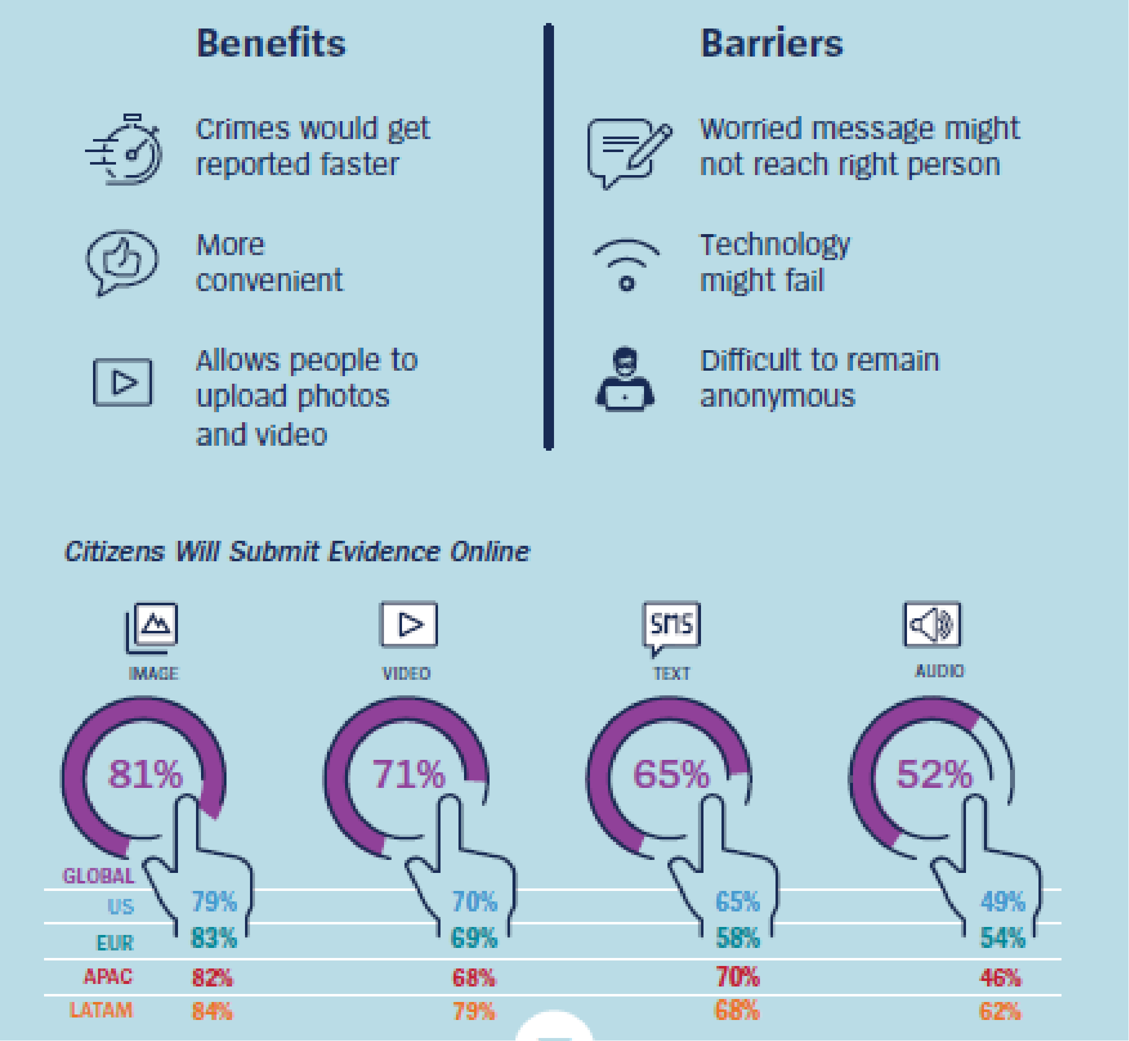


1 Citizens want communication with police to be easier, faster, and more convenient

It should be a lot easier for people to contact the police through digital media

2 Citizens would be more willing to report crime if they could do so via social media

Interacting with Police through Digital Media



Benefits

- Crimes would get reported faster
- More convenient
- Allows people to upload photos and video

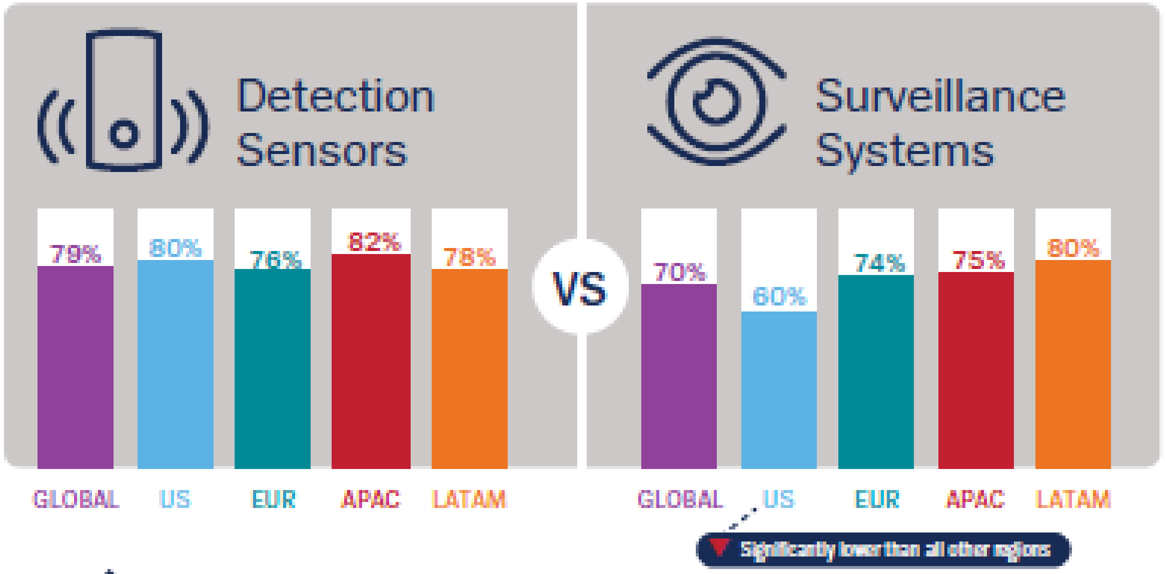
Barriers

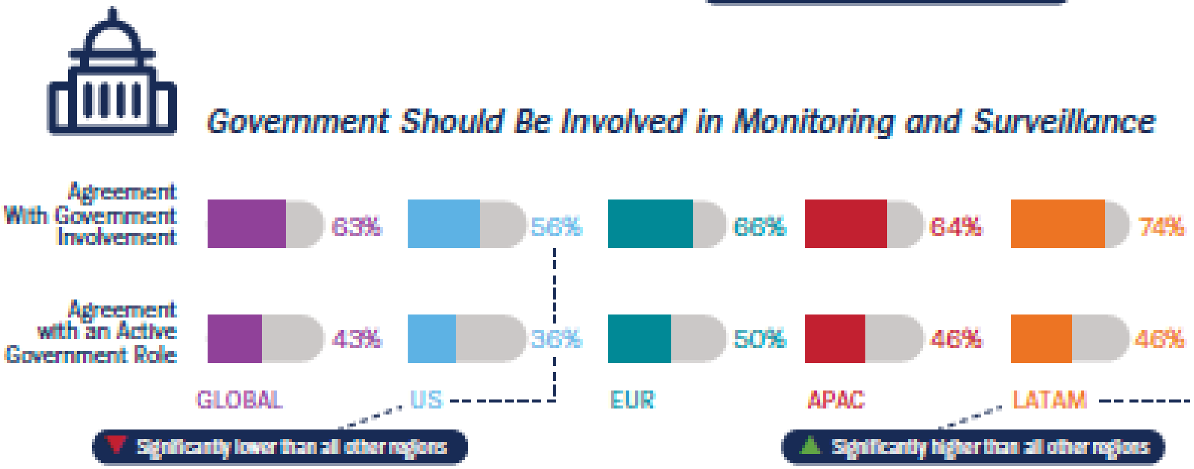
- Worried message might not reach right person
- Technology might fail
- Difficult to remain anonymous

Citizens Will Submit Evidence Online

	IMAGE	VIDEO	TEXT	AUDIO
GLOBAL	81%	71%	65%	52%
US	79%	70%	65%	49%
EUR	83%	69%	58%	54%
APAC	82%	68%	70%	46%
LATAM	84%	79%	68%	62%

Comfort with Technologies for Public Safety - Systems

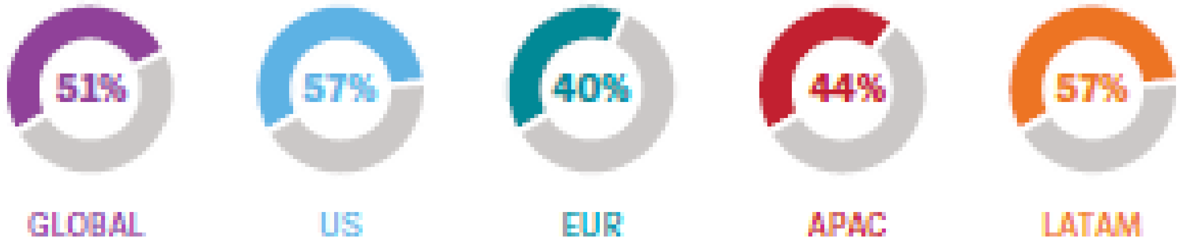




UNISYS | Securing Your Tomorrow®

Comfort with Technologies for Public Safety – Personal, Trust

Collection and use of personal data by law enforcement violates my personal privacy

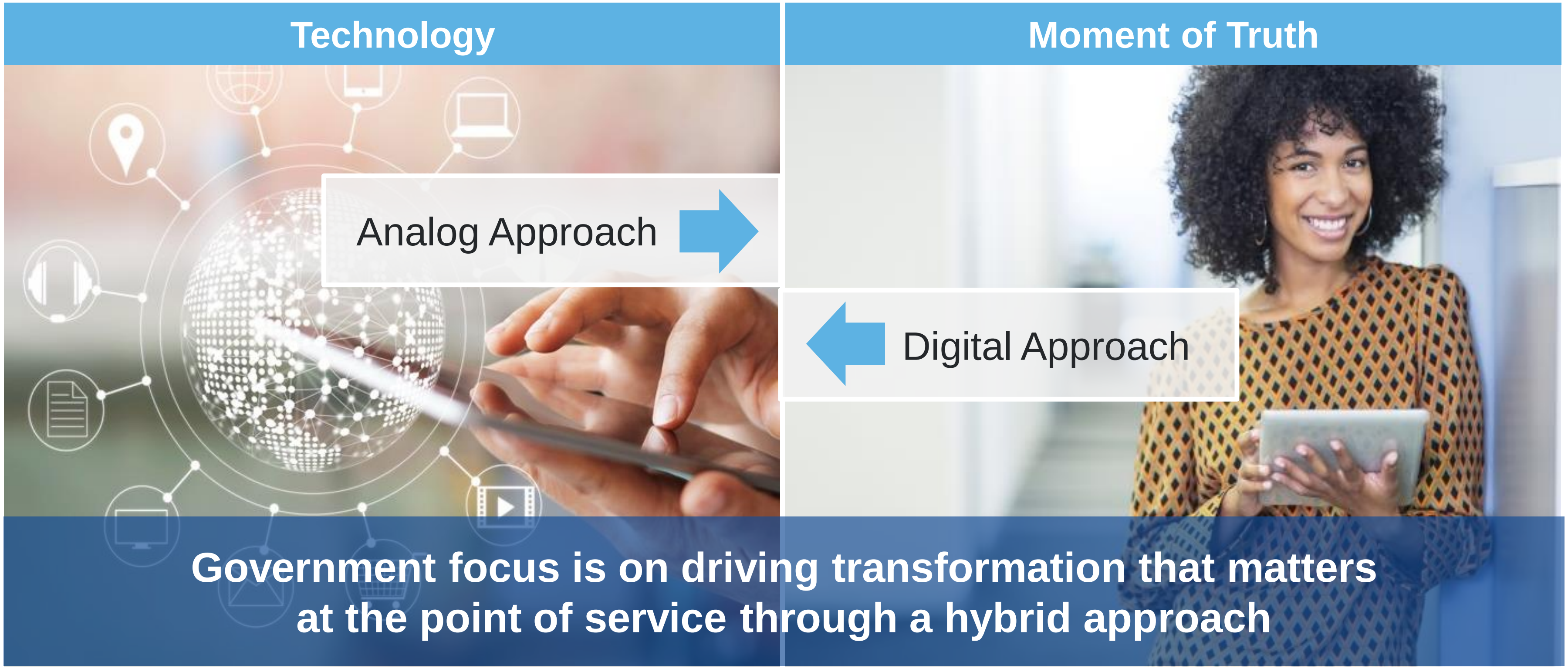


Trust level is greater for government than private entities

	GLOBAL	US	EUR	APAC	LATAM
Government	32%	33%	31%	47%	17%
Private entity	26%	27%	23%	28%	27%

▲ Significantly higher than all other regions

Changing Needs of Digital Citizens



Technology

Moment of Truth

Analog Approach

Digital Approach

Government focus is on driving transformation that matters at the point of service through a hybrid approach

Digital Transformation Outcomes

SHARED SERVICES

BECOME SECURE

ANYTIME ANYWHERE

TRANSPARENCY