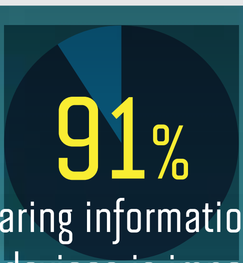
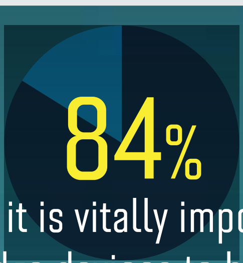
Taming the IoT Frontier

A Federal Framework for Securing the Internet of Things

Is the rate at which agencies adopt the Internet of Things (IoT) outpacing their ability to secure their devices? Government Business Council (GBC) conducted an in-depth research study in January 2017, collecting the perspectives of government decision makers about the security of data at the edge.



91% say sharing information from remote devices is important to executing their agency's mission

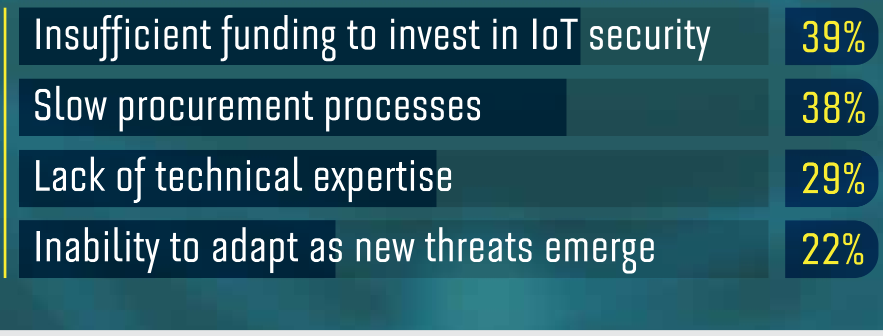


84% believe it is vitally important for such edge devices to be secure

Furthermore...

●●●○ **3 in 4** respondents believe the IoT should be as tightly secured as core infrastructures, capable of adapting as threats grow more sophisticated

Top Challenges to Improving IoT Security



Insufficient funding to invest in IoT security	39%
Slow procurement processes	38%
Lack of technical expertise	29%
Inability to adapt as new threats emerge	22%

In light of these challenges, respondents largely favor a framework that would accelerate security assurance of IoT devices by inviting competition from commercial vendors. However, 64% are unaware that such a program already exists in the **NSA's Commercial Solutions for Classified (CSfC)** program.

Ultimately, while respondents overwhelmingly favor securing the edge, they lack a cohesive path forward. It's time for a change.

Respondents show ample support for a program like CSfC that enables:

- More rapid deployment of automated security updates and vulnerability patches ▶ **81%**
- Agencies to continue protecting most sensitive data with in-house solutions while shielding sensitive-but-less-critical data with commercial solutions ▶ **71%**
- Creation of a standardized application program interface (API) allowing agencies to tailor IoT solutions according to their security needs ▶ **69%**

For a broader exploration of these results,

read more about the report here

bit.ly/2m6wRqW

G Government Business Council

BROCADE