CYBER RESILIENCE:
BUILDING CITIZEN TRUST
Much discussion around government cybersecurity today revolves around the risk of losing sensitive data or perhaps even having data manipulated in harmful ways. These are certainly top-of-mind concerns for government leaders and they should be.

But what sometimes gets lost in these conversations is something far more fundamental to government: citizen trust. As more government activities transpire across digital channels, citizen trust in those activities can become increasingly fragile and fleeting if the public’s belief in their security is shaken.
The government is investing billions of modernization dollars to deliver more services and execute more missions digitally. But to be successful, government agencies must have trust from the citizenry that those digital operations are secure, safe, and authentic. Without that trust, basic government functions—whether taking a census, issuing Social Security cards and benefits, collecting taxes, holding elections, or managing health care—will be questioned and put in peril. Moreover, the effectiveness and efficiencies that modern, digital capabilities promise to deliver will similarly be put at risk.

The fundamental problem is that the Internet today is flawed. When it was developed during the Cold War, the Internet was intended to serve as a reliable communications network for sharing data. It was never designed to accommodate today’s levels of complexity, connectivity, and demand. The Internet’s designers never imagined the degree to which their creation would become embedded throughout the world’s critical infrastructures. It was never designed to operate in the highly sophisticated cyberthreat environments we see today or will encounter tomorrow. Security concerns back then focused on preventing physical failures of the Internet, not on data breaches or harmful manipulations of industrial control systems.

---

**Without that trust, basic government functions—whether taking a census, issuing Social Security cards and benefits, collecting taxes, holding elections, or managing health care—will be questioned and put in peril.**
Today, the emergence of the Internet of Things (IoT) is vastly expanding the Internet’s attack surface. Identities are difficult to authenticate; data integrity is difficult to confirm.

Unless government leaders take effective action, there is a real danger that today’s federal IT modernization investments and efforts will be undermined by an erosion of public trust.

But what actions are needed?

There are two broad categories in which federal leaders can take action. One category concerns the technological, engineering, and design steps needed to ensure that federal IT modernization efforts result in platforms and systems that are highly secure and, even better, resilient to cyberattacks. The other category includes governance, strategies, operating models, and policies that set the direction and standards for cyber behaviors and activities.

In a recent paper entitled “Securing the Digital Economy: Reinventing the Internet for Trust,” two of Accenture’s leading cybersecurity thinkers—Omar Abbosh and Kelly Bissell—discuss these steps at length as they relate to the global community of CEOs. Abbosh and Bissell refer to the technological and engineering steps, which tend to be unseen, as occurring “below ground,” while the standards and governance pieces, which are more visible, are occurring “above ground.”
Many of the same steps that Abbosh and Bissell outline for CEOs apply just as well to government leaders.

“Above ground,” federal leaders can take steps such as:

- **Helping to provide governance and set standards** for how the global community approaches and responds to security threats in a collaborative way

- **Establishing minimum security standards** for IoT-related devices in the global marketplace

- **Leading international conversations** over how individuals, organizations, and nations should be expected to behave on the Internet and install response mechanisms when codes of conduct are violated

- **Crafting standards** for protecting people’s digital identities and even empower citizens themselves as active participants in that process

- **Promoting policies and practices** that promote better sharing of information about cyberattacks
“Below ground,” federal leaders can:

- **Ensure security is baked** into the designs, architectures, and applications they embrace in their modernization efforts.

- **Achieve cyber resilience** by anticipating and preparing for problems by designing assets to: be difficult to attack, minimize impact and potential loss when an event happens, and continuously deliver the intended capability—no matter what.

- **Ensure** that devices throughout their networks—and especially near the edge—are designed to accommodate continuous security updates.

- **Leverage software-defined networking**, which makes network pathways harder to find and attack.

- **Embrace cloud technologies** that harness the ability of elastic workloads, multizone computing, and multi-cloud strategies to fend off adversaries.

- **Apply artificial intelligence** and security automation and orchestration tools to detect and act at machine speed.

By taking the right investments, decisions, and actions today, federal leaders can not only better protect federal operations and reduce the numbers and severity of cyber intrusions, they can also help drive a trust turnaround for American citizens going forward.
About Accenture Federal Services

Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations. Learn more at www.accenturefederal.com.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.