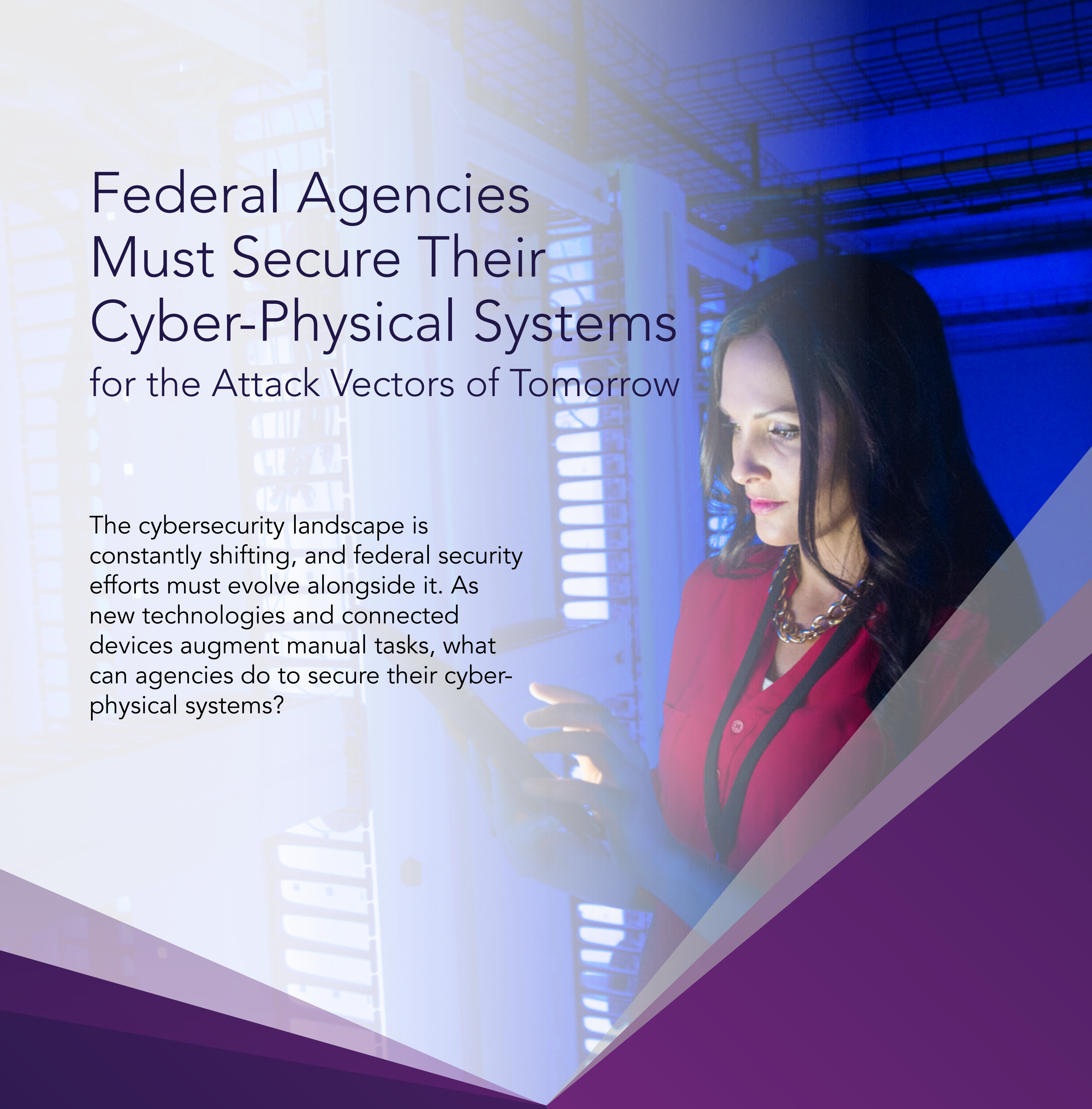


Federal Agencies Must Secure Their Cyber-Physical Systems

for the Attack Vectors of Tomorrow

The cybersecurity landscape is constantly shifting, and federal security efforts must evolve alongside it. As new technologies and connected devices augment manual tasks, what can agencies do to secure their cyber-physical systems?

leidos

The increased convergence between traditional IT infrastructure and cyber-physical systems – from internet-of-things to industrial control systems – is increasing, and it brings increasing risk. In 2021 alone, there were an estimated 12.2 billion active endpoints — and that number will continue to grow, reaching 27 billion by 2025. With the rise of devices connecting wirelessly to networks comes higher data transmission and a wider threat landscape. Securing critical cyber-physical devices is key to keeping citizen and mission data safe, and keeping systems operational.

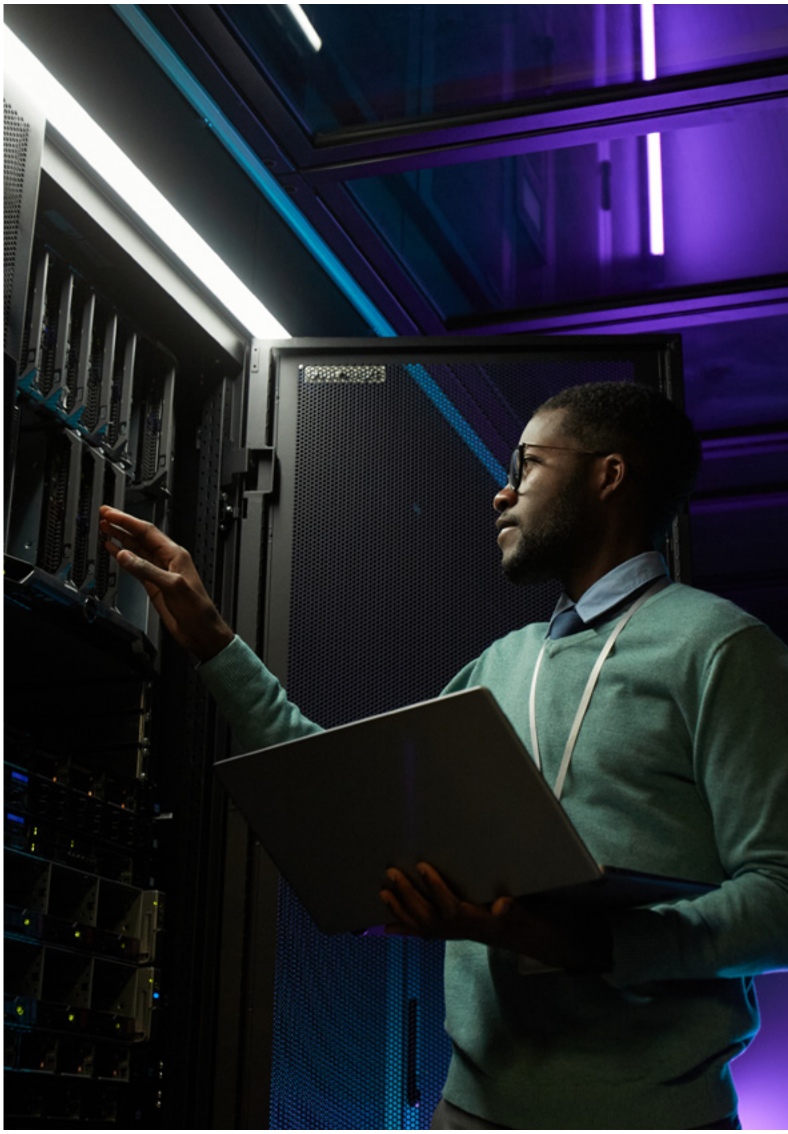
For example: Drones, medical devices, connected fleet vehicles, smart houses, buildings, and cities, as well as supervisory control and data acquisition (SCADA) systems are all cyber-physical systems. Securing them is important to securing our nation's digital infrastructure. Today's threat actors are sophisticated and advanced. So how can agencies ensure they are properly and effectively securing their cyber-physical systems?

As organizations move toward converged network infrastructures that incorporate cyber-physical systems, agencies need to adopt more diverse digital defenses.

This adoption is a herculean challenge, largely due to the legacy infrastructure that runs many of the systems. "The physical infrastructure is significantly different than the IT infrastructure – while IT may be several years old, some cyber-physical is much older, and it must be protected along with very new capabilities. In the same organization, some systems are very advanced and new, and some are quite old and bespoke," says Lexy Guenther, a Leidos cybersecurity expert.

But, with the proliferation of cyber-physical systems across federal IT infrastructures, all the systems are assets agencies must secure. It's about "how do we really drive the right security so that we are. . . enabling this country to succeed while keeping the institutions running?" said Guenther.

Leidos' answer is to help agencies merge their cyber defense protocols and their assets by understanding their cyber-physical space and how to protect it. She continued, "We focus on all the assets as we're doing risk analysis and working with our customers. We bring a holistic approach."



> "In the same organization, some systems are very advanced and new, and some are quite old and bespoke."
>
> —
>
> **Lexy Guenther**
> Leidos Cybersecurity Expert

Every organization has physical elements in their infrastructure, and Leidos combines physical cybersecurity with digital cybersecurity to form a comprehensive solution that works for the agency's enterprise.

To illustrate, think about the energy sector — its infrastructure must remain secure and withstand a possible intentional attack. It must also work one hundred percent of the time. So, security capabilities must be added if and where possible. However, it's also important to secure cyber-physical systems without instilling fear, uncertainty and doubt.

Cybersecurity is a risk-based business, after all. But it's not enough to just secure everything — organizations must understand their most critical assets — those at the highest risk priority – and balance the costs of securing against the priorities of the business or mission. Public sector agencies need a strategy to take effective steps to mitigate risk, and to increasingly reduce their exposure.

Organizations should be asking questions like: Is it essential that this system is continually available? How are the adjacent systems protected if it is attacked? If it goes down, what will be impacted? These questions help identify critical systems, and the connectivity and security they need. Then, organizations can build a strategy around these findings.

"You have to start where your most important assets are and start driving to protect them. That's why you really want to have a strategy, not just an answer," said Guenther. Once the strategy is defined, agencies can determine how their cyber-physical systems fit into

"[Cyber-physical systems]are going to become even more embedded in everything we do, and that means their security will become more and more crucial."

—

Lexy Guenther
Leidos Cybersecurity Expert

their overall IT infrastructure thereby facilitating and supporting the mission.

As Guenther noted, “essential cyber-physical systems must function even during an attack.” They are critical devices to agencies’ missions and operations, so the security around them must withstand threats and allow for human interference during a crisis if needed.

Considering that these systems will become more and more integrated over time, securing cyber-physical systems is a must. Again, Guenther highlighted that “They’re going to become even more embedded in everything we do, and that means their security will become more and more crucial.”

Learn More

about how Leidos is helping federal agencies secure their cyber-physical systems