SAMSUNG

Securing Federal Display Technology

What every IT buyer needs to know

Push
Push
Aapplycation for Naturalization
U.S. Citizenship and Immigration Services
Adress
Ridgefield Park, Bergen Contry, N
Adress 2
Select location
Previous location
Ridgefield Park, Bergen Country, NJ, US
Zip Postal Code : 07660
Wednesday
9 December 2020
17:45
16℃
San Francisco
City Hall
We will be a city hall that strives for better service and faster processing
City Hall service
Civil Petition
Information
TOUCH TO SCREEN

With many Federal employees working from home, agencies are rapidly upgrading to enable video teleconferencing before stopping to consider whether their new technology meets federal security standards.

Samsung is partnering with federal IT professionals to develop and enforce a safer standard for securing large-format displays against cyberattacks.

The new security imperative for digital displays

In the race to digitization, many government officials admit they're not as far along as they'd like to be. According to research from Deloitte, nearly 70 percent of government employees say they're lagging behind the private sector when it comes to digital efficiencies and experiences. People expect government services to be fast, convenient, and personalized—just like consumer services—and agencies are feeling pressure to catch up.

85% of citizens say they expect government digital services to equal or surpass commercial versions.

To meet that need, many agencies are investing in high-definition digital displays and monitors. These displays enable a host of appealing benefits and applications. Some impact internal workflows, from measuring employee productivity to providing rich data visualizations within command and control centers to improving day-today work with high-performance monitors. Other use cases modernize the citizen experience, from helping airline passengers get through TSA lines quicker to providing intuitive, touch-screen options for faster, more convenient trips to the post office.

But perhaps the most common reason agencies are investing in digital displays recently is to facilitate working from home. More than three-quarters of government employees are currently teleworking, and not planning on returning to the office anytime soon.

However, in the wake of the global pandemic, new vulnerabilities in digital technology have arisen. With mobile device usage on the rise and remote work becoming the norm, we've seen a tremendous spike in cyberattacks. As digital connectivity expands, there's more room for cybercriminals to steal private data, disrupt critical services, and damage infrastructure.

Cybercrime on the Rise

In 2020 alone...

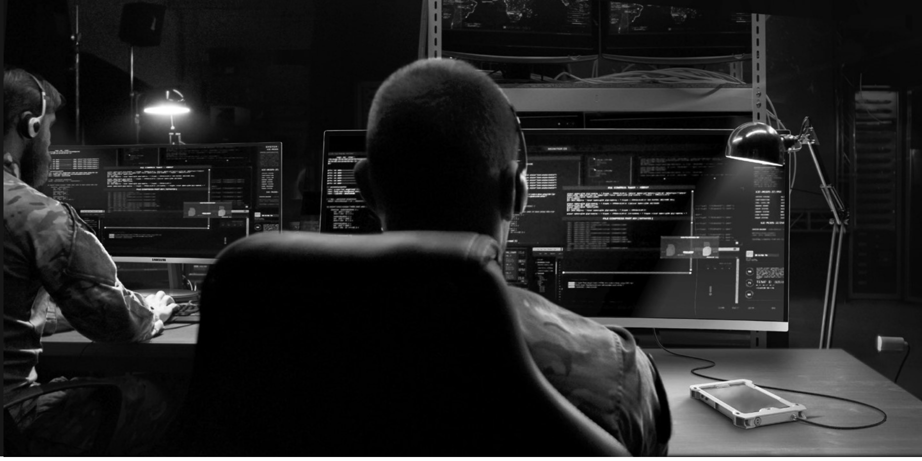
- There was a ransomware victim every 10 seconds
- The U.S. Federal Trade Commission received 1.4M reports of identity theft
- Over 2 million phishing sites were registered by Google—up 27% from the last year.

While government agencies have already established tight security standards for tablets, laptops, networks, and servers, there isn't an overarching standard for large-format displays. With many Federal employees working from home, agencies are rapidly upgrading to enable video teleconferencing before stopping to consider whether their new technology meets federal security standards.

Samsung is partnering with federal IT professionals to develop and enforce a safer standard for securing large-format displays against cyberattacks. What follows are essential security considerations for any Federal agency seeking to adopt digital display technology—either within government workspaces, or as part of the citizen experience.

01

Eliminate unsafe "smart" features



In our connected digital age, consumers want and expect the convenience of wireless connectivity. Features like Wi-Fi and Bluetooth are now built into a range of devices from baby monitors to electric water heaters—and have become all-but-standard on consumer displays, monitors, and screens of all kinds.

But in the context of the Federal Government, these features quickly become vulnerabilities that could compromise everything from confidential files to citizen data to entire network infrastructures. In fact, In 2017, a flaw in a Wi-Fi encryption protocol revealed vulnerabilities that had been accumulating undetected for 20 years.[1] Then, in the Fall of 2020, a newly detected Bluetooth flaw left billions of devices vulnerable.[2]

"Wi-Fi has become something that's included on every device now," says Mike Bahniuk, TKTK. "My speaker bar has Wi-Fi. My garage door has Wi-Fi. But when you get to the agency world, security officers don't want to add additional security to manage. They would prefer displays that have it removed from the core."

That's because despite the convenience of employees being able to connect their devices or presentations wirelessly, displays that have Wi-Fi or Bluetooth built-in become endpoints that hackers can use to gain access to government networks, data, and systems. In response, Samsung has introduced a new line of displays with the latest in high-resolution performance, but without Wi-Fi or Bluetooth.

"Frankly, anything today with an IP address is subject to any kind of security hacks and malware and spam," adds Bahniuk. "Samsung is aware of this and has added a number of different layers to help agencies add to that security protocol."

Additionally, agencies need to avoid so-called "smart" TVs, consumer units designed specifically to connect to outside services like Netflix or iTunes. "As soon as you plug a Smart TV in, it's like you're leaving the back door open," says Bahniuk. "You're communicating with a service that's not secure—and furthermore, employees can download apps that are not secure."

Federal security officers already restrict notebooks from pinging these outside services—and need to start doing the same for displays. Rather than spending time and resources securing or deactivating these types of connected functionalities, agencies should invest in displays and monitors built specifically for federal use that lack these unsafe features altogether.

02

Take a multi-layered approach

There's no silver bullet for stopping bad actors who are intent on accessing government data. That's why it's critical to take a multi-layered approach to security. Rather than employing one or two blockades, like a firewall and two-step identification, building security into applications, platforms, and hardware is essential to preventing attacks.

Additionally, establishing a secure Remote Desktop Protocol (RDP) and secure Virtual Network Computing (VNC) enables physical and remote meeting participants to connect to other network computers and servers through a protected connection. Though we have yet to see a massive-scale attack using home networks as a vector, cybersecurity experts suggest that criminals may be poised to take advantage of less-secure home networks, which lack enterprise-grade firewalls.

To maximize protections against cyberattacks, either within government properties or work-from-home environments, Samsung displays and monitors are secured at multiple levels with our Knox defense-grade security system.

Samsung Knox defense-grade security system

Multi-level security: Isolate, encrypt, and secure your data—from hardware to chip—including confidential files, credit card transactions, and passwords.

Powerful flexibility: Easily secure, deploy, and manage displays for federal use, while allowing employees to stay productive.

Unmatched convenience: Maintain total control of your entire system from a single centralized location.

Best of all, Samsung display solutions (and their accompanying security protocols) are easy to implement—offering quick and simple out-of-the-box device setup, configuration, rebranding, and enrollment for all federal use cases.

03

Meet key certifications

At first pass, you might not think of a digital display as a security vulnerability. We tend to think attacks happen behind the scenes—on servers, storage units, and networks. But as displays proliferate in government, agencies need to ensure security by only adopting devices that adhere to certain key certifications.

Critically, you can't evaluate the security of a display or monitor from the surface. Two displays that look identical from the front end, could tell a different story behind the glass—one might be rife with vulnerabilities, while the other is downright impenetrable. When these devices are used in a federal context, certain certifications need to be upheld to prevent instances of malware, ransomware, spam, phishing or any number of harmful cyberattacks.

The Key Certifications to watch for include:

TAA (United States Trade Agreements Act)

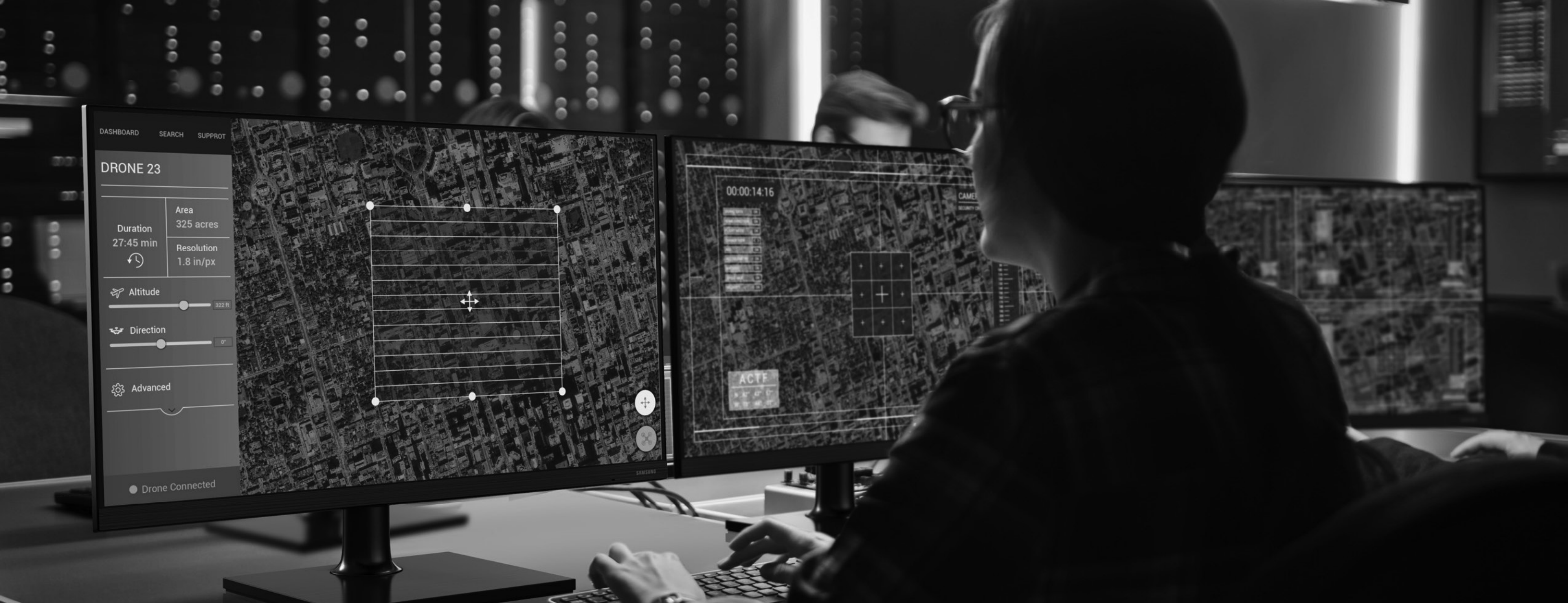
Passed in 1979, the US Trade Agreements Act, or TAA, enables federal agencies to limit procurement to vendors whose goods and services are made exclusively in the United States or a TAA-approved country. This restriction greatly reduces the likelihood of bringing displays and monitors into your organization that have security vulnerabilities built into them.

As a global leader in digital technology, Samsung's products are produced in every corner of the globe. All our displays—especially those designed for government use—come from TAA-approved countries. Not only does this better secure your agency, but it helps speed up the procurement cycle.

Common Criteria

Common Criteria is an international set of security standards for IT products, and the largest of its kind in the world. When digital display technology meets these standards, you can be sure that the process of specification, implementation, and evaluation has been "conducted in a rigorous, standard and repeatable manner at a level that corresponds with its target use environment," per Common Criteria's website. This is an essential certification for all government displays.

All Samsung display solutions are built and installed to meet exacting Common Criteria requirements.



Data screen retention

Before LCD/LED became the dominant display technology, plasma screens were the standard across all industries. But there was a critical security vulnerability baked into the screen itself, known as data screen retention. If content was held on a screen for too long, that data would become etched into the plasma of the display and could be retrieved later. Obviously, if you're displaying classified information, this is a problem.

The latest displays from Samsung have zero screen retention—every pixel of data is wiped once the screen is turned off.

Memory volatility

Despite the negative-sounding name, a device with memory volatility is actually a positive when it comes to cybersecurity. Devices with volatile memory erase data stored in their RAM as soon as the device is turned off. From the most secure levels of government on down, displays with volatile memory are valuable, as they can be deployed at the highest, most classified levels of government.

Samsung Displays feature this memory volatility certification—all RAM memory disappears immediately as soon as power is disconnected.

In addition, Samsung's Knox-protected Federal display solutions allow customization, rebranding, and deployment of fit-for-purpose mobile devices.

In a nutshell, Samsung Knox has successfully met the rigorous security requirements set by governments and major enterprises around the world, providing business users with a robust mobile security solution.

Furthermore, Samsung Displays are Cisco-certified—which means they work securely on Cisco video tele-conferencing (VTC) solutions like Room Kit or WebEx, and it's easy for agencies to integrate these displays into VTC applications and rooms.

Cybersecurity is the White House's number one IT priority for 2021.

If you're an IT leader in the federal government, balancing cybersecurity standards with modern technological needs is on your mind. Samsung can help you integrate this newest layer of technology into your agency infrastructure—and further safeguard your security at the same time.

We continue to sculpt the future of the digital display market by delivering:

- Defense-grade security
- Superior picture quality
- Product diversity
- Customized solutions
- Advanced system-on-a-chip (SoC) technology
- An open-content platform
- Simple-to-use content management

Samsung's digital display ecosystem makes it easy to meet your agency's vision of the future and dramatically improves the civilian experience—all while exceeding federal cybersecurity standards. To experience the power of cutting edge visual displays and state-of-the-art cybersecurity technology, speak with a Samsung representative today.

Footnotes:

[1] https://www.engadget.com/2017-10-16-Wi-Fi-vulnerability-krack-attack.html

[2] https://www.wired.com/story/bluetooth-vulnerability-iran-indictments-security-news/

Learn more

samsung.com/government
insights.samsung.com
1-866-SAM4BIZ

Follow us

youtube.com/samsungbizusa
@samsungbizusa