



Progress Through Regional Cooperation In The Alleghenies

State of the Southern Alleghenies APEX Accelerator - January 2025

by James Gerraughty
SAP&DC APEX Accelerator Program Manager



Happy New Year!

I hope this year brings you peace and joy! We have a lot of items to consider in government contracting: Cybersecurity, FOCI, changes/updates to the PA COSTARS program, SAM...The list goes on. However, this keeps us on our toes in service to our clients and community. As I always say to people who ask me if I like my job, "it's never boring." changes. Speaking of training, please review our training opportunities that are coming up in January 2025 (and beyond for our APEX Accelerator and PREP Partners, once our funding is confirmed). A big one is some entry level NIST 800/CMMC Level 1 training, an introduction to the ERDCWERX program at the U.S. Army, and an update to the PA COSTARS program. You can review and register for upcoming events on our [eCenter page](#). Stop back often, as the training events do update regularly!

Finally, if you have ideas for topics, or would like to learn more about something, please drop us a line at (814) 949-6500 or by [email](#). We'd love to hear from you!

Agencies still struggle with online accessibility, GSA says By Natalie Alms, Staff Reporter, Netxgov/FCW

The federal government is often failing to meet its own requirements for digital accessibility, according to a new, congressionally-mandated report released late last month.

The report notes that in the "26 years since the Rehabilitation Act of 1973 was amended to include Section 508, governmentwide Section 508 conformance remains low."

The law requires that federal technology like apps and websites be accessible to people with disabilities, which make up about 13% of Americans, according to the Census Bureau.

But only a third or less of federal agencies' most viewed tech is fully in line with Section 508 standards meant to ensure accessibility, and governmentwide digital accessibility decreased in fiscal 2024.

The report follows increased attention to the issue in recent years, although "digital accessibility remains largely deprioritized across government," it notes.

The Office of Management and Budget updated guidance on Section 508 for the first time in a decade in 2023, and the Justice Department issued a final rule with standards and requirements for digital accessibility on the state and local level last spring.

Congress laid down requirements for this GSA report in 2022, following over a decade of the DOJ not issuing its own, congressionally-mandated report on Section 508 compliance in the federal government. [Continue Reading](#)

(Accessed 1/9/2025)

Parents think schools' cybersecurity is stronger than reality, report says
By Chris Teale, Managing Editor, Route Fifty

Recent research from Keeper Security found a “widening gap” between the perception of districts’ cyber readiness. Better training and information sharing can help improve the outlook.

The closing months of 2024 saw more cybersecurity issues at some of the nation’s public-school districts, as administrators had to recover from cyberattacks and the exposure of student and staff data.

Students in Providence, Rhode Island, had their personal data exposed in a hack, including their vaccination records and driver’s license information. Meanwhile, an attack in Wayne County, Michigan, shut down one school system’s internet and phone service, leaving officials scrambling to restore it.

The costs are enormous, too. A report from Comparitech last year found that schools and colleges on average lose \$500,000 a day from ransomware attacks. Governments have been slowly responding, whether it be some states now requiring that incidents be reported to officials, or the Federal Communications Commission kicking off a \$200 million pilot program to provide schools and libraries grants to boost their cybersecurity.

And new research has highlighted the urgent need for schools to improve their cybersecurity posture and the gaps in awareness. A survey by cybersecurity software company Keeper Security released late last year found that while 74% of parents expressed confidence in the cybersecurity measures of their children’s schools, only 21% reported receiving guidance on secure password management and cyber hygiene. [Continue Reading](#)

(Accessed 1/9/2025)

GAO mulls cost evaluation of nationwide telecom hardware replacement
By David DiMolfetta, Cybersecurity Reporter, Netxgov/FCW

One major vulnerability exploited by China’s Salt Typhoon hacking unit is a Cisco hardware flaw that can’t be patched and requires physical replacement, according to a person with knowledge of the intrusions.

The nation’s top oversight office is considering penning a study to assess the cost of administering a far-reaching operation to rip out and replace swaths of at-risk or compromised telecommunications equipment owned by small communications providers around the country, according to a senior U.S. official.

The deliberations, which have not been previously reported, are fueled by an ongoing Chinese espionage intrusion into U.S. and allied telecommunications networks by Salt Typhoon, a hacking unit tied to Beijing’s Ministry of State Security that likely had unfettered access to key elements of America’s telecommunications backbone for around two years.

As part of the work, the U.S. Government Accountability Office would study the costs of undertaking such a project and, separately, would also evaluate security vulnerabilities impacting the telecommunications industry, said the official, who spoke on the condition of anonymity because they were not authorized to discuss the private deliberations.

Should President-elect Donald Trump’s national security team support this study, it could motivate his allies in Congress to greenlight what would likely be a multi-billion dollar effort to weed out troves of telecommunications hardware that’s been accessed or is at risk of being ensnared by Chinese hackers and other adversaries. [Continue Reading](#)

(Accessed 1/9/2025)

About US

The Southern Alleghenies APEX Accelerator at SAP&DC is an economic development entity that bridges the gap between supplier and buyer in the government marketplace. The APEX Accelerator stands ready to support businesses in the central PA Alleghenies region in the pursuit to secure contracts with local, state and/or federal government agencies nationwide.



Due to the generous support of our Commonwealth and Federal funding partners, services provided by the APEX Accelerator are free of charge.

Whether you are an experienced contractor or new to the government marketplace, the APEX Accelerator will provide one-on-one counseling utilizing all of the program resources necessary to increase your share of contract awards. We will also coordinate assistance, if needed, with our PA PREP partners.

Contact us today at the Southern Alleghenies APEX Accelerator at SAP&DC to get started!

Email: apex@sapdc.org

Phone: (814) 949-6500

Web: [APEXAccelerator@SAP&DC](http://www.sapdc.org)

SAP&DC is an Equal Opportunity Employer

SAP&DC | 814-949-6528 | jgerraughty@sapdc.org | <http://www.sapdc.org>
3 Sheraton Drive
Altoona, PA 16601



SAP&DC | 3 Sheraton Drive | Altoona, PA 16601 US

[Unsubscribe](#) | [Constant Contact Data Notice](#)



Try email marketing for free today!