Modernizing Physical and Digital Security in Government

Thank you for downloading this Security Information Systems (SIS) resource. Carahsoft is the dealer and distributor for SIS Cybersecurity solutions available via GSA Schedule 70, NASA SEWP V, ITES-SW and other contract vehicles.

To learn how to take the next step toward acquiring SIS's solutions, please check out the following resources and information:

For additional resources:
carah.io/SISResources

For upcoming events:
carah.io/SISEvents

For additional Forescout solutions:
carah.io/SISSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
securitysoftware@carahsoft.com
(844) 445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/SISContracts

Modernizing Physical and Digital Security in Government

Upgrading security systems is more important than ever. Here is how agencies can do so while meeting budget constraints.

Security systems in both the physical and digital realms of work are evolving and increasing in complexity. As piecemeal systems proliferate, there is increasing demand for unified solutions that deliver necessary insights through a single pane of glass. In this fast-growing and complex landscape, government agencies need to figure out how to upgrade their security defenses while working with legacy equipment and keeping an eye on the budget.

The State and Local Security Landscape

Spurred by changes in the way we work and an increasing clamor for efficiencies in all aspects of commercial building management, both physical and digital security systems are evolving rapidly. While such growth is exciting, government agencies face challenges when modernizing these critical systems.

› **Legacy technologies.** While a rip-and-replace solution might give agencies leading-edge capabilities, it is not a practical strategy for those that have brownfield systems in place.

"A big challenge is that these physical assets might have electronic security systems with varying degrees of modernity," says Eric Young, senior vice president of operations for Security Information Systems (SIS), a provider of alarm monitoring and interface services for the security industry.

Workarounds to accommodate legacy systems have created a patchwork of solutions for many agencies. "These systems often don't talk well with each other," Young says. "They are often siloed due to age and compatibility and proprietary versus open-source solutions."

› **Geographically dispersed assets.** Because agencies might have a presence across many different buildings in an area, security also needs to spread out across physical entities and assets on the ground. When you are only as safe as your weakest link, vulnerabilities multiply and it can be difficult to triage security leaks. "There might be a security operations center (SOC) that uses cameras and monitors buildings using an intrusion alarm system but if they are not co-located, that becomes a very complex problem," Young says.

› **Physical and digital security are coming under one umbrella.** When they do so, operational technology (OT) from physical assets has to seamlessly integrate with information technology (IT). If there is dissonance between infrastructure, software and monitoring, teams are frequently burdened with too much repetitive or unnecessary information.

› **Competitive labor market.** Operating complex security systems needs a deep bench of talent that might not always be available in house. Contractors need solutions that are easy to work with.

The Advantages of Modernization

Given this complex security landscape and its many challenges, it is time for government agencies to modernize their physical and digital security systems. A modernized security system integrates all security solutions, physical and digital, and delivers monitoring capabilities through a single pane of glass. Doing so offers a range of benefits, including:

› **Situational awareness across all systems physical and digital.** If a location shuts down, agencies still need to be able to monitor it from another location to ensure business continuity. "Also, if there is an anomalous activity or attack at one entry point, I can immediately look for similar activity across the network," Young says.

› **Integration across various kinds of software and physical systems.** Unified solutions ensure IT and OT work together. They cover gaps in security and decrease data redundancy so employees can focus on relevant alerts that matter the most and work on remediation efforts as quickly as possible.

› **Centralized security protocols so everyone can work with one pane of glass.** The problem with scattered security operation centers is that they often lead to fragmented responses and siloed information. There is no unified chain of command despite the fact that security bugs can easily hop from one location to another. Integrated and centralized systems establish better lines of communication and help eliminate silos.

› **Decreased labor costs.** There are 360,000 cybersecurity jobs left unfilled at the state, local and federal government levels.[1] Integrating and centralizing security solutions helps get more out of existing personnel without having to worry about finding the right talent at multiple locations.

Factors to Look for When Modernizing Security Systems

Government agencies looking to modernize their security systems might want to consider the following factors.

› **Compatibility.** The proposed solutions need to work with existing legacy systems instead of simply being a rip-and-replace model. "Compatibility with heterogeneous systems is key because you might encounter a variety of open-source and proprietary solutions; a modern security solution needs to make all of them talk," Young says.

› **Customization.** Since agencies all have varying needs and requirements, it's important that solutions be easily customized. Partners also need to understand the intricacies of integrating physical and digital security as the field is constantly evolving. Agencies need professionals who understand the mechanics underlying security while delivering an elegant and easy-to-use solution. "Systems have to be tailored to fit the way the client operates. They need to make decision-making as easy as possible," Young says, adding that jazzy dashboards are not always the answer.

"The convergence of physical and digital security has begun and government agencies need a partner who can work with their legacy systems, meet a budget and deliver a central pane of glass for actionable insights."

Eric Young, Senior Vice President of Operations, SIS

› **Extensibility.** Questions agencies should ask include: Will the solutions work with technologies coming down the pike? Can we add new capabilities at a later date? Agencies do not want to be locked into a security solution that does not have room to grow.

What the Future Holds

The future is going to be more about integrating the physical and digital realms of security technology. Getting started on the path to modernization will be key to managing this change effectively.

"The convergence of physical and digital security has begun and government agencies need a partner who can work with their legacy systems, meet a budget and deliver a central pane of glass for actionable insights," Young says. "That future is now."

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from SIS Evercommerce.

Endnote

1. https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: SIS

Security Information Systems, Inc. (SIS) is a global leader with over 30 years of experience in alarm monitoring & integration solutions for the security industry. Seamlessly integrate with over 100 third-party systems while continuously monitoring and automating responses to all alarm signals for fast and accurate event management. For more information on SIS, please visit: **securitysoftware.com or call 407-345-1550**