Agenda

All Times Are EDT

SIA GovSummit Agenda

May 21st, 2024

7:30am–8:30am

Breakfast Available/Registration Begins (Exhibits Open)

Where: Atrium

Check in for GovSummit at our registration desk, enjoy breakfast and networking with other event attendees and stop by our exhibitor tables.

8:30am–8:35am

Welcome and Opening Remarks

Where: Auditorium

Don Erickson

CEO

Security Industry Association

8:35am–9:00am

Day 1 Keynote: Kris Cline, Director, Federal Protective Service

9:00am–9:30am

SIA Awards Presentations

Where: Auditorium

SIA will present the 2024 SIA Women in Biometrics Awards, SIA Excellence in Government Service Awards and Industry Advocate Awards.

9:30am–10:15am

Navigating the Digital Transformation in Physical Access Control

Where: Auditorium

In this panel discussion, participants from large enterprises and multinational technology companies deep in the government vertical market will share their experiences and insights on the digital transformation of physical access control. We will explore how the industry has

evolved into an enterprise software industry, the challenges and opportunities this change presents and how to keep up with fast-paced technology changes and a dynamic landscape. This session will provide greater insights on 1) the impacts of digital transformation on the physical access control industry and it influences the way the industry functions, builds, sells, implements and operates, 2) best practices for implementing high assurance credentials in onsite, cloud and hybrid architectures and 3) lessons learned when high assurance and a high level of convenience are needed.

Eric Dean

Chief Technology Officer, Security and Electronic Systems

M.C. Dean

Derek Greenland

Director, Federal Government Solutions

LenelS2

Jeff Nigriny

CEO

CertiPath

Lee Odess

CEO

Access Control Executive Brief

10:15am–10:45am

Networking Break (Exhibits Open)

Where: Atrium

Enjoy coffee, network with other GovSummit attendees and stop by our exhibitor tables during this break.

10:45am–11:15am

High Security and Access Control: Best Practices in Government Security

Where: Auditorium

What do high security and access control in the government sector really mean? There are stringent requirements for the types of credentials allowed to be used by federal employees in highly sensitive positions. Traditionally, these employees have relied on various types of PIV cards; however, many federal employees don't fall into this classification – such as office staff, janitorial staff, patients in VA hospitals or faculty, staff and students at schools run by the federal government. These individuals have historically been provisioned run-of-the-mill plastic cards that can be insecure and difficult to manage.

These higher-risk proximity cards can be transitioned to Bluetooth-based mobile credentials to make accessing federal buildings easier and more secure, and Bluetooth Low Energy technology can be used for secure reader configuration; however, there is significant hesitance to use a Bluetooth technology in the government sector, despite the potential benefit of newer solutions such as mobile credentials.

Additionally, there are a host of physical access control solutions on the market. SIA Open Supervised Device Protocol-supported access control systems can communicate and exchange data securely and efficiently, ensuring only authorized individuals can access certain areas – and therefore preventing unauthorized physical access and potential security breaches; however, not all systems are created the same. Cards can now also contain embedded authorization, which allows users to digitally verify against a federal repository for that credential holder.

This panel will explore these newer access control technologies, cover best practices in access control for the government sector while maintaining federal standards and address the questions audiences need to be asking to inform their government security decisions and select the right solution for them. The session will also work to overcome the myth that "Bluetooth is bad" and educate attendees on what is allowed in the government sector in terms of Bluetooth and mobile credentials. Attendees will have the opportunity to ask questions during a Q&A portion following the panel.

Daniel Clark

Physical Security Representative

U.S. Department of Veterans Affairs

Phil Coppola

Business Development Director for Mobile Solutions – PACS North America

HID

Michael Hamilton

Government End User Business Development Manager

HID

Trevor Hoselton

Director of Business Development

HID

Dale Gigandet

Director of Strategic Programs

Allied Universal Technology Services

3:45pm–4:30pm	A New Era of American Investment in a Deglobalized World: What It Means for Supply Chains and Procurement Rules ×

Where: Auditorium

For the last 40 years, globalization and worldwide supply chains have been a major priority across industries and have dominated economic trends; however, a drive for greater domestic industrial bases coupled with post-COVID-19 pandemic effects causing supply

We have laws and regulations for gun ownership, active shooter education and training, and security technologies to deter, detect, delay and deny an active shooter from committing an act of gun violence.

This presentation will discuss the terminology and statistics used to describe mass shootings

11:15am–12:00pm	New Federal Initiatives for Protecting Crowded Spaces +
12:00pm–1:00pm	Networking Break/Lunch (Exhibits Open) +
1:00pm–1:45pm	Disability Access in Emergency Operations Planning for Schools +
1:45pm–2:30pm	Public-Private Partnerships and the Future of Protecting High-Risk Minority Communities +
2:30pm–3:00pm	Networking Break (Exhibits Open) +
3:00pm–3:30pm	Risk Mitigation for School Campuses and Government Facilities Using Ballistic Safe Places +
3:30pm–4:00pm	One School's Quest to Secure Their School, Through +