SECURE
TECHNOLOGY
ALLIANCE

How to Plan, Procure & Deploy a PIV-Enabled PACS

Access Control Council Webinar Series

Session Two: Facility Characteristics & Risk Assessment

Introductions

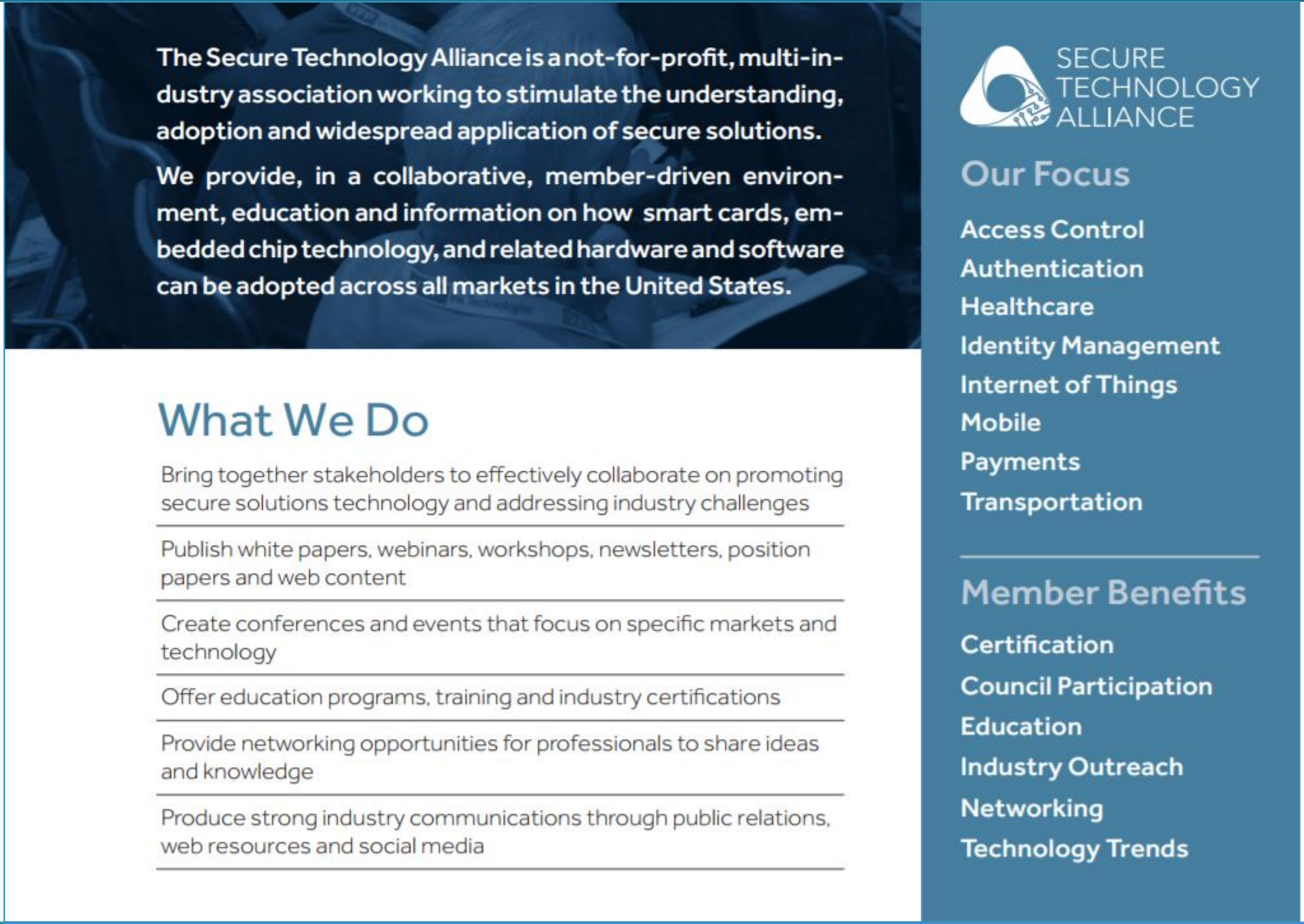
Randy Vanderhoof, Secure Technology Alliance

Lars Suneborn, Secure Technology Alliance

Michael Kelley, Parsons Corp.

William Windsor, Department of Homeland Security

Who We Are



The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

- Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

SECURE TECHNOLOGY ALLIANCE

Our Focus

- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

Member Benefits

- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

Access Control Council

… focuses on **accelerating** the widespread **acceptance, use, and application of secure technologies** in various form factors **for physical and logical access control**. The group brings together, in **an open forum**, leading users and technologists **from both the public and private sectors.**

COUNCIL RESOURCES

White Papers

- Commercial Identity Verification (CIV) Credential: Leveraging FIPS 201 and the PIV Card Standards
- A Comparison of PIV, PIV-I and CIV Credentials
- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance Summary
- FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems
- FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience
- Guide Specification for Architects and Engineers for Smart Card-based PACS Cards and Readers for Non-government PACS
- Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses
- PIV Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide
- Smart Cards and Biometrics
- Strong Authentication Using Smart Card Technology for Logical Access
- Supporting the PIV Application in Mobile Devices with the UICC

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

National Center for Advanced Payment and Identity Security

National Center for Advanced Payments and Identity Security

- **National Center for Advanced Payments and Identity Security** in Crystal City
- **Secure Technology Alliance Educational Institute** is part of the center.
- **Certifications Available**
  - **CSCIP**
  - **CSCIP/Payments**
  - **CSCIP/Government**
  - **CSEIP**

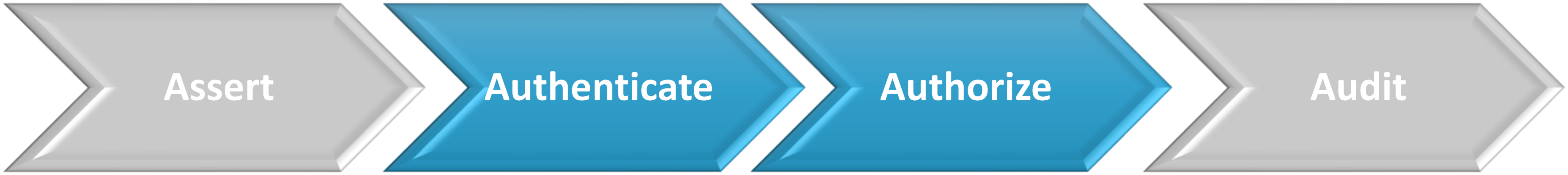
What constitutes compliance?

Secure and reliable forms of identification:

- are issued based on sound criteria for verifying an individual employee's identity
- are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- can be rapidly authenticated electronically
- are issued only by providers whose reliability has been established by an official accreditation process

"The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application"

- Homeland Security Presidential Directive 12



Assert

Authenticate

Authorize

Audit

The PIV-Enabled PACS Process

Session Five

Session Two

Facility Characteristics

- Size
- Mission
- Assets
- Existing Conditions
- Regulatory Requirements

Risks

- Threats
- Likelihood
- Consequence

Session Three

Scope

- Risks to be mitigated
- Costs and timelines
- Potential solutions
- Potential providers

Session Four

Procurement Strategy

- Responsibilities
- Standards
- Procurement vehicles
- Contract documents
- Funding
- Evaluation
- Award

Session Five

Deployment

- Management
- Design
- Installation and configuration
- Testing and acceptance
- Training
- Cutover
- Close out

Facility Risk Assessment Guidance

- The Risk Management Process for Federal Facilities: An Interagency Committee Standard (https://hsin.dhs.gov/Pages/home.aspx)
  - Executive Branch agencies must use per E.Os 12977 and 13286
  - Adopted by DoD in 2012 and Integrated into Unified Facilities Criteria (UFC) 4-010-01) DoD Minimum Antiterrorism Standard for Buildings
  - Factors for assessing facility risk
    - Mission Criticality
    - Symbolism
    - Facility population
    - Facility size
    - Threat to agency

- ASIS International Risk Assessment Standard ANSI/ASIS/RIMS RA.1-2015 (https://www.asisonline.org/Standards-Guidelines/Standards/Pages/default.aspx)

Asset Identification and Criticality

What assets are you protecting?

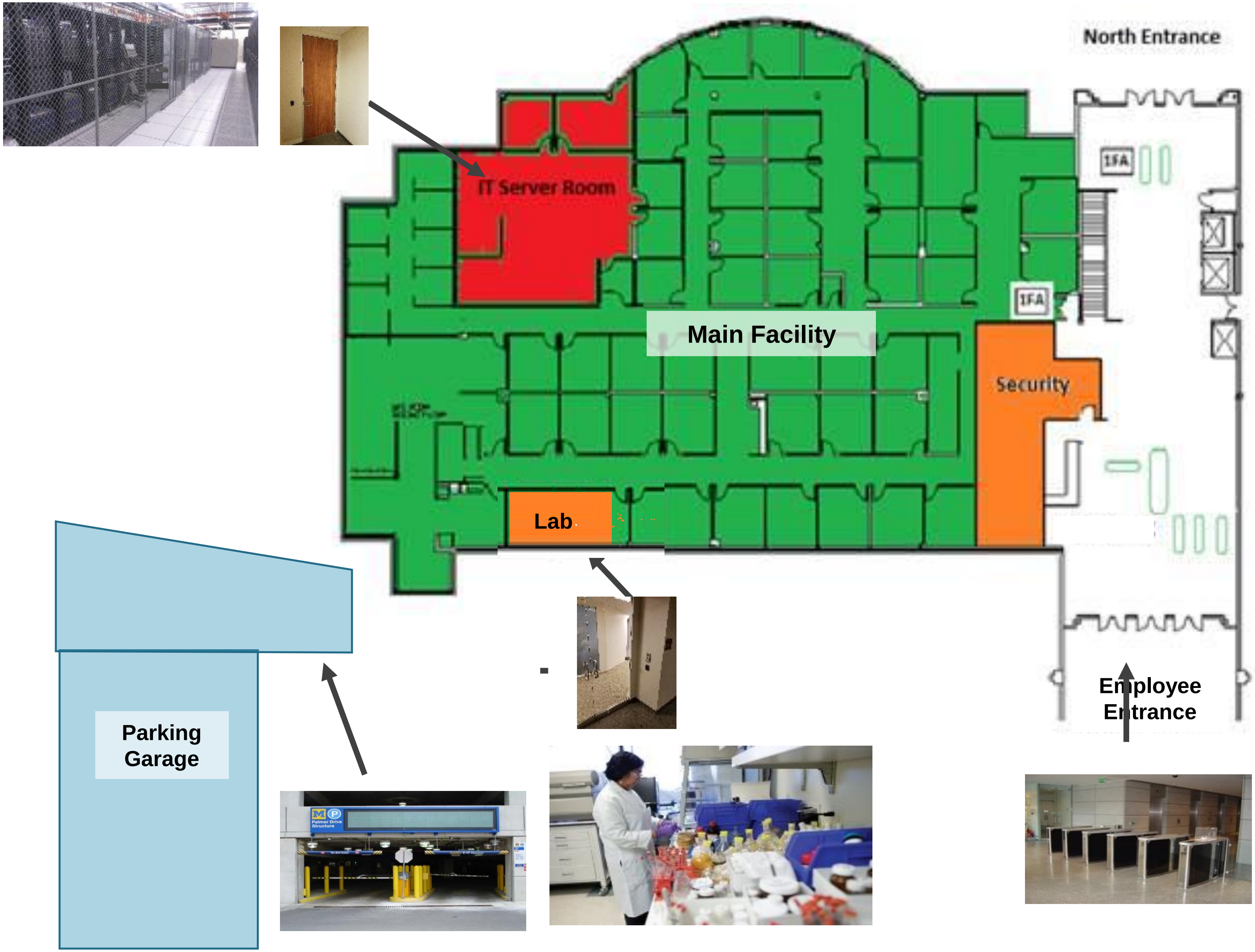
- Facilities
  - Campus, building, garage, storage facility, armory, suite, room
  - Leased or owned (directly managed or through another agency)
  - Single or multi-tenant occupied
  - Environmental factors (terrain, adjacent facilities)
- Equipment, Materials and Information
- Asset Value

What impacts are you trying to mitigate?

- Inability to perform critical/essential functions
- Productivity loss
- Personal safety threats
- Repair or replacement cost
- Confidence or reputation loss

Correlation of Mission, Assets & Protection

- Public access
- Administrative
- Data processing
- Communications
- Medical
- Transportation
- Maintenance
- Law enforcement
- Intelligence
- Critical infrastructure



Main Facility

Lab

Parking Garage

Employee Entrance

Asset Locations and Threats

Where are the assets you are protecting?

- Geographic location of the facility
  - Similar events nearby
  - Accessibility to potential adversaries
- Location of assets within the facility
  - Selection of authentication mechanisms

What & Whom are the assets being protected from?

- Threat types
  - Natural
  - Man-made (Human initiated)
- Threat factors
  - Tenant perception
  - Nature of the mission
  - Threats to the federal agency
  - Threats to other tenants of a facility
  - Local factors i.e. crime statistics

Adversaries

- Adversary Motivation
  - Money
  - Ideology
  - Coercion
  - Ego
- Adversary Capabilities
  - Tactics
  - Funding
  - Knowledge
  - Tools, materials or special skills
- Appendix A ISC Design-Basis Threat Report (https://hsin.dhs.gov/Pages/home.aspx)

PACS Assessment

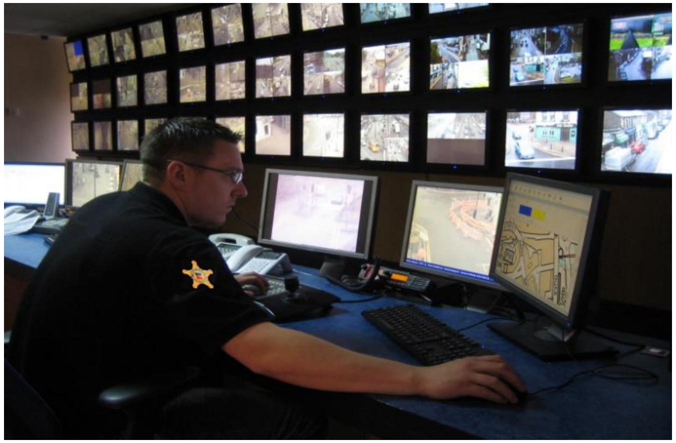
How are you ***currently*** protecting your assets?

- Begin at the perimeter and work inward
  - Physical barriers
  - Vehicle and personnel access control points
  - Demographics
- PACS lifecycle
  - Age and condition
  - Hardware, firmware and software versions
  - Supporting infrastructure
  - Authority to Operate (ATO)
- Integrated systems
  - Surveillance
  - Intrusion detection
  - Elevator control
  - Fire alarm
  - Command and control

PACS Effectiveness

Does the ***existing*** PACS …

- electronically authenticate credentials fast enough for the throughput?
- deny access to individuals presenting revoked, lost, stolen, expired, cloned, altered or otherwise fraudulent credentials?
- deny access to individuals with valid credentials but no proper authorization?
- accurately detect events?
  - invalid card, access denied, door held, door forced, equipment tamper, power or communications failure
- properly annunciate events to responding personnel in a timely manner?
- support multifactor authentication?



Legal and Regulatory Requirements

- Federal Laws
  - Federal Information Security Modernization Act of 2014, P.L. 113 – 283
  - Privacy Act of 1974, 5 U.S.C. § 552a
  - Americans with Disabilities Act of 1990, 42 U.S.C. § 12101
- State and local laws
  - May impose additional requirements, i.e. licensing and permits
  - Varying applicability
- Agency Regulations
  - Include requirements from other agencies, i.e. OMB, GSA, NIST, DHS
  - Specific asset requirements
- Best Practices and Guidelines
  - NIST
  - ISC
  - Secure Technology Alliance
  - ASIS International
  - Security Industry Association

Risk = Probability x Consequence

1. Identify Threats *

A. Criminal Activity

B. Explosive Event

C. Ballistic Attack

D. Unauthorized Entry

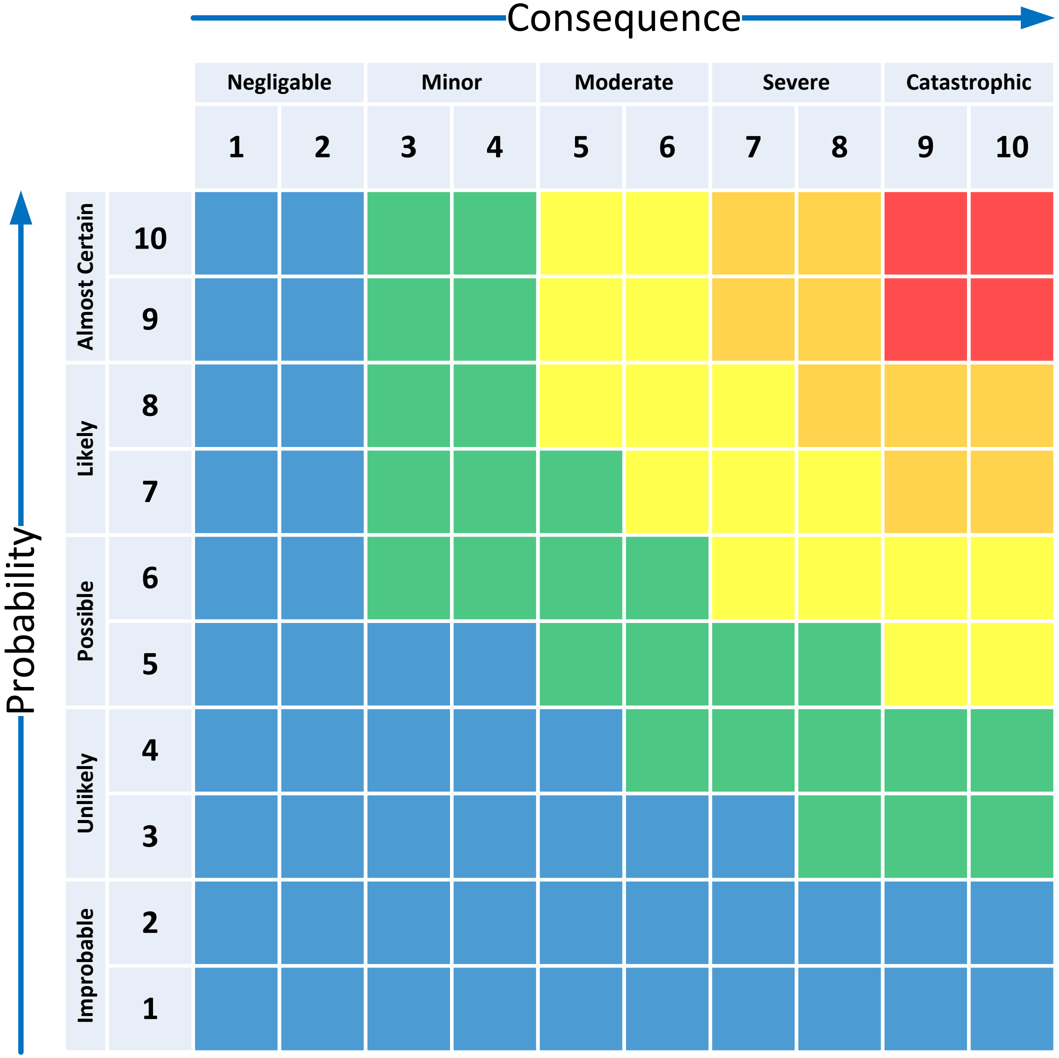
E. CBR Release

F. Vehicle Ramming

G. Hostile Surveillance

H. Cyber Attack

I. UAS Attack



		Negligable		Minor		Moderate		Severe		Catastrophic	
		1	2	3	4	5	6	7	8	9	10
Almost Certain	10	🟦	🟦	🟩	🟩	🟨	🟨	🟧	🟧	🟥	🟥
	9	🟦	🟦	🟩	🟩	🟨	🟨	🟧	🟧	🟥	🟥
Likely	8	🟦	🟦	🟩	🟩	🟨	🟨	🟨	🟧	🟧	🟧
	7	🟦	🟦	🟩	🟩	🟩	🟨	🟨	🟨	🟧	🟧
Possible	6	🟦	🟦	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨
	5	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟨	🟨
Unlikely	4	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩
	3	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩
Improbable	2	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
	1	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

* From Appendix A ISC Design-Basis Threat Report – For Illustration Only

Risk = Probability x Consequence

2. Rank Threat Probability

D. Unauthorized Entry
H. Cyber Attack
A. Criminal Activity
G. Hostile Surveillance
C. Ballistic Attack
F. Vehicle Ramming
B. Explosive Event
I. UAS Attack
E. CBR Release

Consequence →

↑ Probability

		Negligable		Minor		Moderate		Severe		Catastrophic	
		1	2	3	4	5	6	7	8	9	10
Almost Certain	10	D	🟦	🟩	🟩	🟨	🟨	🟧	🟧	🟥	🟥
	9	H	🟦	🟩	🟩	🟨	🟨	🟧	🟧	🟥	🟥
Likely	8	A	🟦	🟩	🟩	🟨	🟨	🟨	🟧	🟧	🟧
	7	G	🟦	🟩	🟩	🟩	🟨	🟨	🟨	🟧	🟧
Possible	6	C	🟦	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨
	5	F	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟨	🟨
Unlikely	4	B	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩	🟩
	3	I	🟦	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩
Improbable	2	E	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
	1	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

Risk = Probability x Consequence

3. Rank Threat Consequence

H. Cyber Attack - 45

C. Ballistic Attack - 42

B. Explosive Event - 36

D. Unauthorized Entry - 30

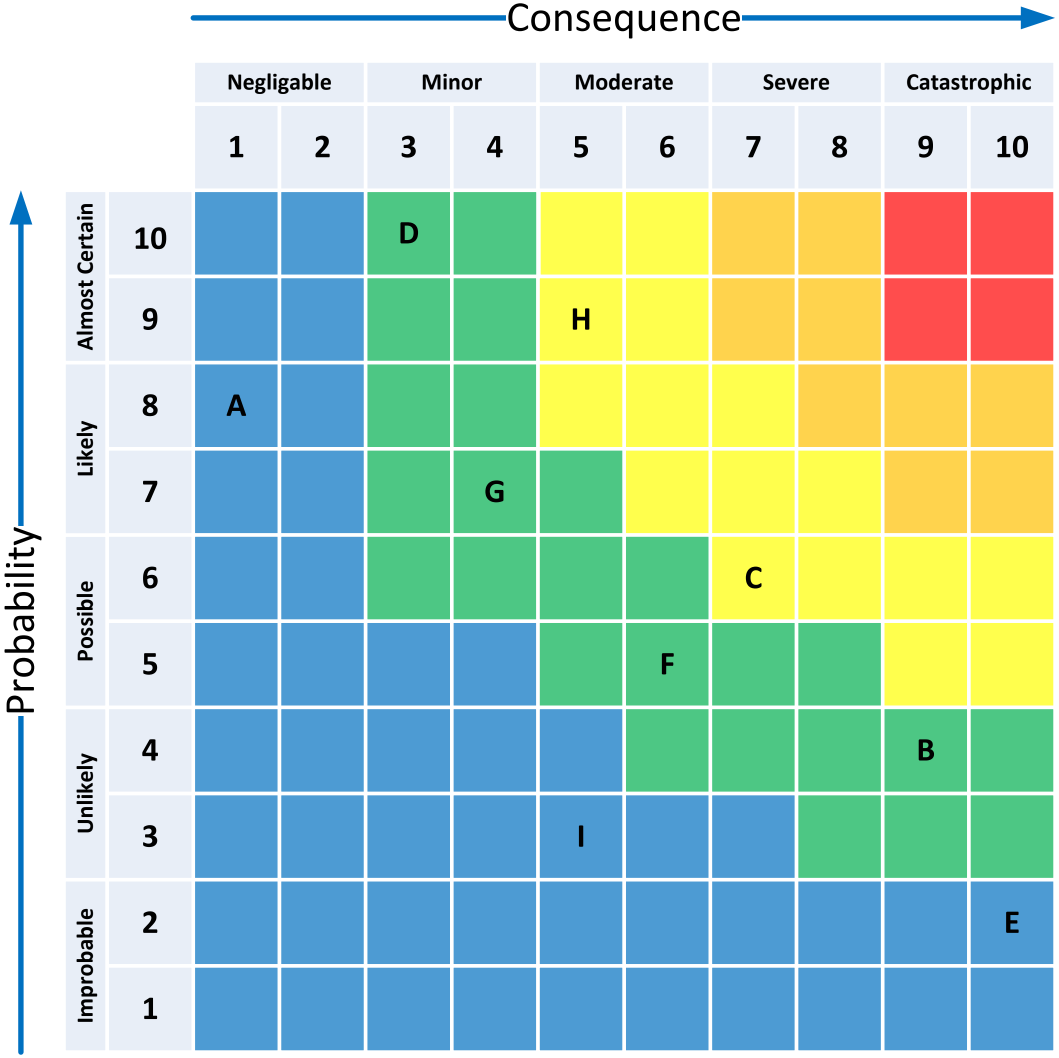
F. Vehicle Ramming - 30

G. Hostile Surveillance - 28

E. CBR Release - 20

I. UAS Attack – 15

A. Criminal Activity - 8



		Negligable		Minor		Moderate		Severe		Catastrophic	
		1	2	3	4	5	6	7	8	9	10
Almost Certain	10	🟦	🟦	🟩 D	🟩	🟨	🟨	🟧	🟧	🟥	🟥
	9	🟦	🟦	🟩	🟩	🟨 H	🟨	🟧	🟧	🟥	🟥
Likely	8	🟦 A	🟦	🟩	🟩	🟨	🟨	🟨	🟧	🟧	🟧
	7	🟦	🟦	🟩	🟩 G	🟩	🟨	🟨	🟨	🟧	🟧
Possible	6	🟦	🟦	🟩	🟩	🟩	🟩	🟨 C	🟨	🟨	🟨
	5	🟦	🟦	🟦	🟦	🟩	🟩 F	🟩	🟩	🟨	🟨
Unlikely	4	🟦	🟦	🟦	🟦	🟦	🟩	🟩	🟩	🟩 B	🟩
	3	🟦	🟦	🟦	🟦	🟦 I	🟦	🟦	🟩	🟩	🟩
Improbable	2	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦 E
	1	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

Risk Mitigation

Risk cannot be eliminated, only reduced

- Countermeasures
  - Appendix B Countermeasures (https://hsin.dhs.gov/Pages/home.aspx)
- Reduce consequence
  - Redundancy
  - Insurance
- Reduce likelihood
  - Restrict access to sensitive areas/materials
  - Require higher levels of identity and authentication assurance
    - *Digital Identity Guidelines*, NIST Special Publication 800-63-3 (https://csrc.nist.gov/publications/)
  - Select appropriate authentication mechanisms
    - *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, NIST Special Publication 800-116 (https://csrc.nist.gov/publications/)

Upcoming Sessions

- Establishing the Project Scope – January 11, 2018
- Developing the Procurement Strategy – February 22, 2018
- Implementing the Solution – March 15, 2018
- Use Cases and Lessons Learned – April 19, 2018

All webinars begin at 2 p.m. ET/11 a.m. PT.

Visit the Secure Technology Alliance web site to register for a session or to watch the recording of any previous session.

Upcoming Sessions

Stakeholders	Session 1 10/19/2017	Session 2 11/30/2017	Session 3 1/11/2018	Session 4 2/22/2018	Session 5 3/15/2018	Session 6 4/19/2018
Acquisition	♦		♦	♦		♦
Budget	♦		♦	♦		♦
Customers / Tenants	♦	♦	♦		♦	♦
Engineering	♦				♦	♦
Executive Sponsors	♦	♦	♦	♦	♦	♦
Facility Management	♦	♦	♦		♦	♦
Information Technology	♦		♦		♦	♦
Legal	♦	♦		♦		♦
Personnel	♦		♦		♦	♦
Physical Security	♦	♦	♦	♦	♦	♦
Safety	♦	♦			♦	♦

Resources and Contacts

http://www.securetechalliance.org

Lars Suneborn, CSCIP/G, CSEIP

Director, Training Programs, Secure Technology Alliance

lsuneborn@securetechalliance.org

Michael Kelley, CSCIP/G, CSEIP, PSP, CBP

Principal ESS Technical Specialist, Parsons Corp.

michael.p.kelley@parsons.com

William Windsor, CSEIP

Department of Homeland Security

william.windsor@hq.dhs.gov

SECURE
TECHNOLOGY
ALLIANCE

191 Clarksville Road
Princeton Junction, NJ 08550