BUILDING
Cyber Security

Advancing Physical Security, Safety, and Privacy

Approach

Establish and administer a framework offering market-driven options created by physical cyber secure stakeholders to improve physical citizen security, safety & privacy.

The BCS Framework is focused on increasing the asset value, while facilitating incentives for the comprehensive enhancement of technology, processes, & training to respond to a rapidly, evolving global threat.

Problem

- **Known & Expanding Threats to Physical Safety**
  Critical infrastructure, utilities, facilities, schools, homes
- **Widening Range of Interfaces**
  Artificial intelligence, machine learning, robots, smarter technologies, automation
- **National Intelligence**
  Compromised control system list growing & posing national risk
- **Increasing Sophistication of Bad Actors**
  Increasing sophistication of bad actors (nation-state, terrorists, criminals, hackers)

Threat Information Actionable/Consumable

Stakeholders with Risk

- Smart device vendors/installers
- Building operators
- Building owners
- Control systems manufacturers
- Insurance companies
- Cyber services companies

Current Risk Mitigation (limited)

- Cyber rating assessments
- Hire cyber defense companies to run systems
- Gov't regulatory policy
- Cyber standards organization non-coordination
- Engineering improvements/investments
- Educate/Train (Cyber Hygiene, Awareness)

CURRENT DATA, SOFTWARE, PC'S PROTECTION

NEW PHYSICAL THREAT OF CONTROL SYSTEMS

Security Framework

BUILDING Cyber Security

Framework Comparison

Proposed BCS	ISA/IES 62443	DoD Model	DoE Maturity (C2M2)	NIST Tier Model
● Bronze	Maturity 1	Basic	Level 0	Partial
● Silver	Maturity 2	Intermediate	Level 1	Risk Informed
● Gold	Maturity 3	Good	Level 2	Repeatable
● Platinum	Maturity 4	Proactive	Level 3	Adaptive
		Advanced		

BCS seeks to harmonize existing government frameworks and convert for private industry adoption

Standards Consolidation
Consolidation of standards already in public domain

Dynamic Threat
Framework designed to provide value for entire system lifecycle due to evolving threat

Adaptive Model
Framework will evolve to meet changing threats

Recertification
Evolving threat environment requires on-going education

Assessment
Provide parameters for third party assessment of facilities based on framework scoring metrics

Tenant Rating
Public or private - Owner discretion

EXTERNAL STAKEHOLDERS

Insurance Companies

Seeking an accepted market standard by which to graduate levels of coverage and fees for clients

Rating Agencies

Recognize the threat to citizen safety and devices in real estate; Will look for a market standard to reinforce its company ratings to mitigate lawsuit threats and negative publicity

Mortgage Lenders

Will look for levels of physical cyber security as they currently look for fire/life/safety compliance