BUILDING Cyber Security

Cyber IGE

Society of SAME American Military Engineers

www.buildingcybersecurity.org

Oct 26, 2021

Agenda

- Review of the IGE Charter
- Receive a brief introduction of the BCS framework
- Discussion of IGE milestones and deliverable
- Identification and assignment of initial IGE Working Group tasks
- Establish Rhythm for PT meetings
- Plan for delivery of update to a CEO Roundtable to be held at the SAME Small Business Conference in Atlanta on Wednesday, Nov 17 at 3pm

Feel Free to ask questions at any point during the meeting

BUILDING Cyber Security

IGE Charter

Mission

- **Increase understanding and mitigate cybersecurity risks to physical infrastructure and facilities owned and/or operated by federal agencies**
- **Identify ways that SAME can support federal agency partners in mitigating those risks.**

Key Focus Areas :

- **Identify/evaluate OT related risks to federal missions, assets, and personnel**
- **Cultivate cyber risk subject matter expertise both in industry and federal agencies**
- **Engage leading experts in protection of OT in building management systems**
- **Engage the facility engineering team in federal agencies**
- **Develop content in support of federal policy development**

Proposed updates to targeted documents, starting with specifications (UFGS) and criteria (UFCs) related to Control System Cybersecurity UFC (UFC 4-010-06) and UFGS (UFGS 25 10 10) as well as of the UFCs and UFGS for HVAC controls and Utility Monitoring and Control Systems.

- https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06
- https://www.wbdg.org/ffc/dod/unified-facilities-guide-specifications-ufgs/ufgs-25-10-10

BUILDING Cyber Security

IGE Charter

Deliverables:

- ❑ White Paper on Reducing Cyber Risk in Smart OT for Federal Facilities and Infrastructure
  - Discuss risks associated with use of smart OT in federal facilities (awareness, thought leadership)
  - Discuss potential cyber risk mitigation strategies (awareness, thought leadership)
  - Curated list of best practices for securing smart OT for federal facilities and infrastructure (awareness)
  - Proposed framework for analyzing risk and the criticality of mitigating vulnerabilities (awareness, advocacy)
  - Design review checklist for protection of smart building management systems. (awareness)
  - Recommended changes to applicable policies and specifications as informed by best practices (advocacy)

BUILDING Cyber Security

IGE Charter

Proposed Milestones:

- ✓ Kickoff Panel – DC/NoVA Post Meeting – 16 Sep 2021
- ✓ Charter approved and IGE Working Group established Oct 20, 2021
- ✓ Commencement of IGE activities – Oct 26, 2021
- ❑ Vector Check – SBC CEO Roundtable – Nov 2021
- ❑ White Paper Preview at NOVA/DC Post public event – Apr 2022
- ❑ White Paper Submission to SAME Executive Committee – JETC – May 2022

SAME's Executive Committee may consider extending and/or expanding the PT to address ongoing or emerging cyber issues or initiatives.

BUILDING Cyber Security

Building Cyber Security

Our Mission

Establish and sustain frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization offering market-driven options to promote cyber protections in controls and devices for enhanced physical security and safety in an increasingly smart world.

Our Vision

Building Cyber Security (BCS) will be the premier global administrator certifying operational technologies, processes, training, and recovery plans for safe, secure use of controls and devices.

BUILDING
Cyber Security

CRE Cyber Risk Include Both OT & IT

OT

PHYSICAL SYSTEMS

- HVAC
- Lighting
- Access Control
- Parking
- Video Surveillance

BUILDING TECHNOLOGY

- Building Management
- Building Automation
- IOT/Sensors

IT

INFORMATION TECHNOLOGY

- Mission Systems
- NIPR/SIPR/JWICS
- AI, ML, Military Data

BUILDING Cyber Security

Framework Goals & Requirements

GOAL: Establish an OT cybersecurity risk management framework and conformance certification scheme that uses a market-driven approach for incentivizing stakeholders across the building technology lifecycle to improve physical cyber safety, security, and privacy while assuring the mission.

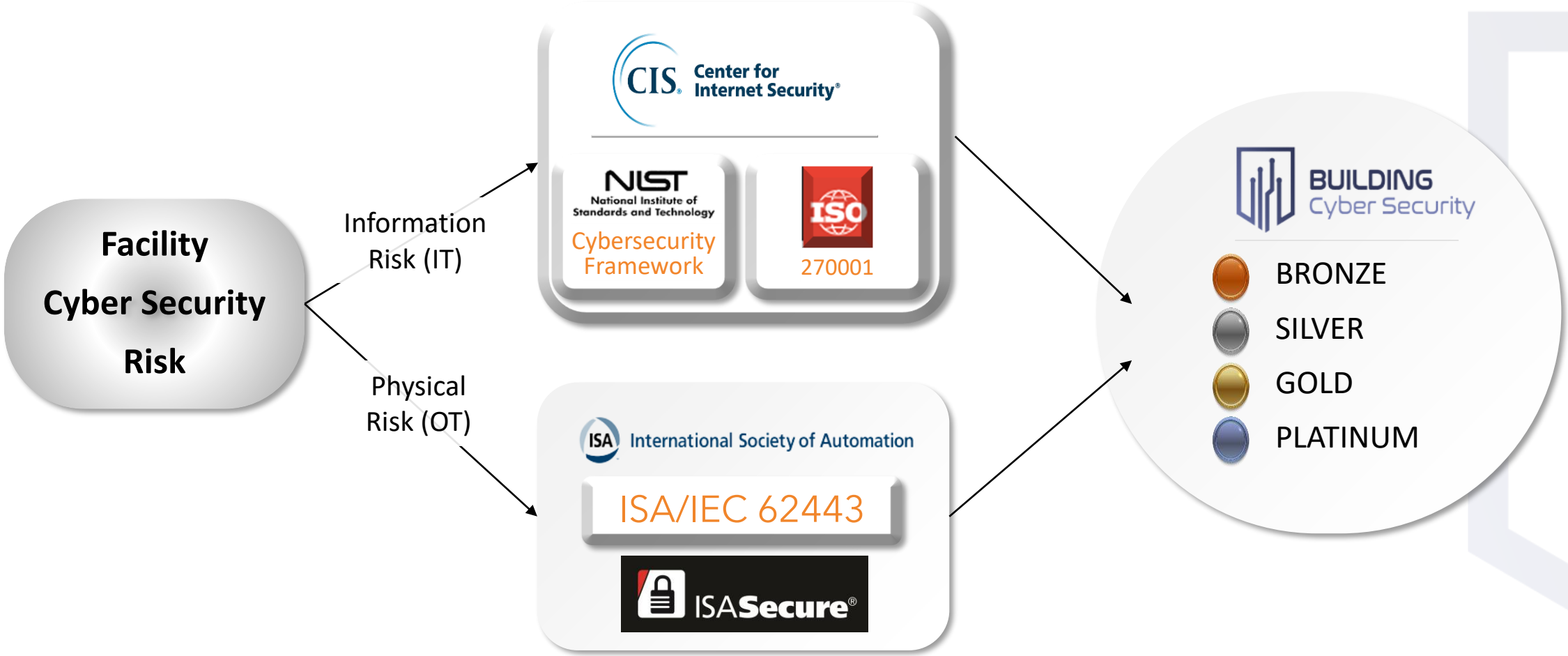
Required Outcomes	Guardrails
• Safety, security, and privacy of people and mission assurance	• Leverage existing technical standards and avoid duplication
• Risk prioritization for owners/operators to protect buildings, campuses, cities from cyber-physical threats	• Ensure framework is modular and enduring to keep pace with technology and regulatory change
• Translation of physical cyber improvements to incentives*	• ***Includes building OT and IT that supports/interfaces with OT***
• Enable tools to perform safe-active assessments of building OT	• Excludes enterprise IT systems/services independent of OT
• Share common issues & trends with broader community	

Deliverables

1. Risk framework
2. Certification & labeling scheme
3. Profiles

*Possible incentives: liability protection, purchasing preference, insurance benefits, tax incentives, etc.. save X% on insurance … reduce outages by Y% … reduce data loss occurrences by Z%

BCS Framework Leverages Existing Standards and Controls



BCS RATING SCHEMA

		Bronze	Silver	Gold	Platinum
OT Zones	Essential Function Zones	62/90 (69%)	83/90 (92%)	90/90 (100%)	90/90 (100%)
	Standard Zones	56/85 (66%)	77/85 (91%)	85/85 (100%)	85/85 (100%)
	Process Maturity Level	Repeatable	Repeatable	Repeatable	Improving
IT Zone	**CIS Implementation Group**	**IG1**	**IG2**	**IG3**	**IG3**

*BCS rating is based on the lowest score between OT and IT scoring.

BUILDING Cyber Security

Discussion of IGE milestones and deliverables

Ideas?

Identification/assignment of IGE Working Group tasks

Written Sections of White paper (Lead and Support)

1. Discuss risks associated with use of smart OT in federal facilities (awareness, thought leadership)
2. Discuss potential cyber risk mitigation strategies (awareness, thought leadership)
3. Curated list of best practices for securing smart OT for federal facilities and infrastructure (awareness)
4. Proposed framework for analyzing risk and the criticality of mitigating vulnerabilities (awareness, advocacy)
5. Design review checklist for protection of smart building management systems. (awareness)
6. Recommended changes to applicable policies, criteria, and specifications as informed by best practices (advocacy)

Rhythm of Meetings

BUILDING Cyber Security

Cyber IGE CEO Roundtable

Goal is to provide senior engineering industry leader review and guidance for the work of the SAME Project Team

- ❑ Discuss the range of cyber threats and risk for SAME Stakeholders
- ❑ Review the charter, deliverables, and timelines
- ❑ Receive input from attendees on focus and deliverables

To be Held at the SAME CEO Roundtable at SBC Wednesday, Nov 17 from 3-5 pm

BUILDING Cyber Security

BUILDING Cyber Security

brian.may@buildingcybersecurity.org

Lucian@buildingcybersecurity.org

Society of SAME American Military Engineers