

Business Plan

Updated: September 2020

# Mission

To establish and sustain a framework administered by a non-profit organization that offers market driven options developed by a broad range of stakeholders for “Cybersecure” to improve physical security, safety and privacy in both public and private facilities and related infrastructure.

# Vision

The framework will accelerate the comprehensive enhancement of technology, processes and training to respond to a rapidly evolving global cyber threat.

# Definition of Problem

The internet has transformed the daily lives of most people around the globe. The total installed base of connected devices Internet of Things (IoT) is projected to amount to 75 billion worldwide by 2025, a fivefold increase in ten years.1.

Connection between devices has even expanded into mechanical systems in commercial buildings, such as elevators and HVAC systems, which use embedded computers to connect and report. This increased connection has led to tremendous operational efficiencies, but, unfortunately, has also led to mounting vulnerability to cyber attack.

In years past, many of the cyber threats focused on “hacking” into systems to access valuable personal credit card and identity information. Today, cyber threats are expanding into more traditional, “operational technology”, or OT systems, and are now able to cause physical harm to citizens and assets. The rapid growth of “IoT” technology into all spheres of society is increasing the attack surface.

Currently policies and programs designed to address this threat are fragmented and difficult for stakeholders to understand. Many standards and best practices for these OT systems already exist, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the International Electrotechnical Commission/International Society of Automation series of standards on security for industrial automation and control systems (IEC/ISA 62443). These standards and best practices, however, are extremely technical and do not translate easily into a common set of standards to building owners and operators.

In addition to the standards not being easily understood, the current publicly available threat intelligence information is beyond the understanding of most Americans.

1 <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

# A Different Approach

Create a non-profit, market driven, special purpose entity to translate complicated standards and threat intelligence information into consumable and actionable information.

Key representatives from both the private and public sector can, working together, accelerate and sustain the necessary and appropriate cyber defense actions.

This entity will have a positive impact by:

* **Educating** stakeholders in interpreting standards and best practices for their organizations
* **Creating** the framework for the Cyber Performance Ratings across the levels of “cybersecure”

by:

* + Interpreting the current standards and define a holistic approach to cyber vulnerability risks that applies to a specific stakeholder group.
  + Determining their exposure and their ability to secure their assets

Developing a transparent “cyber risk rating”. Framework will allow end userso be able to choose their levels of exposure to cyber threats

* + Allowing the insurance industry to use ratings for tiering of relevant systems to end users
* **Sustaining** the framework to educate and continually update the ecosystem on threat exposure and defense ability
* **Performing assessments** and testing on assets to rate that individual asset and/or organization

#### Assess and Issue a Cyber Performance Rating

* Based on consolidation of standards already in public domain
* Dynamic threat – the threat is always evolving
* Dynamic response – the program for the response is always evolving
  + Incentivizes sustainment of good cyber practices over life cycle
  + Dynamic – rating requires periodic recertification to sustain these good cyber practices
* Assessment addresses protections of technology, processes, and people
* Rating public or private tenants – Owner discretion

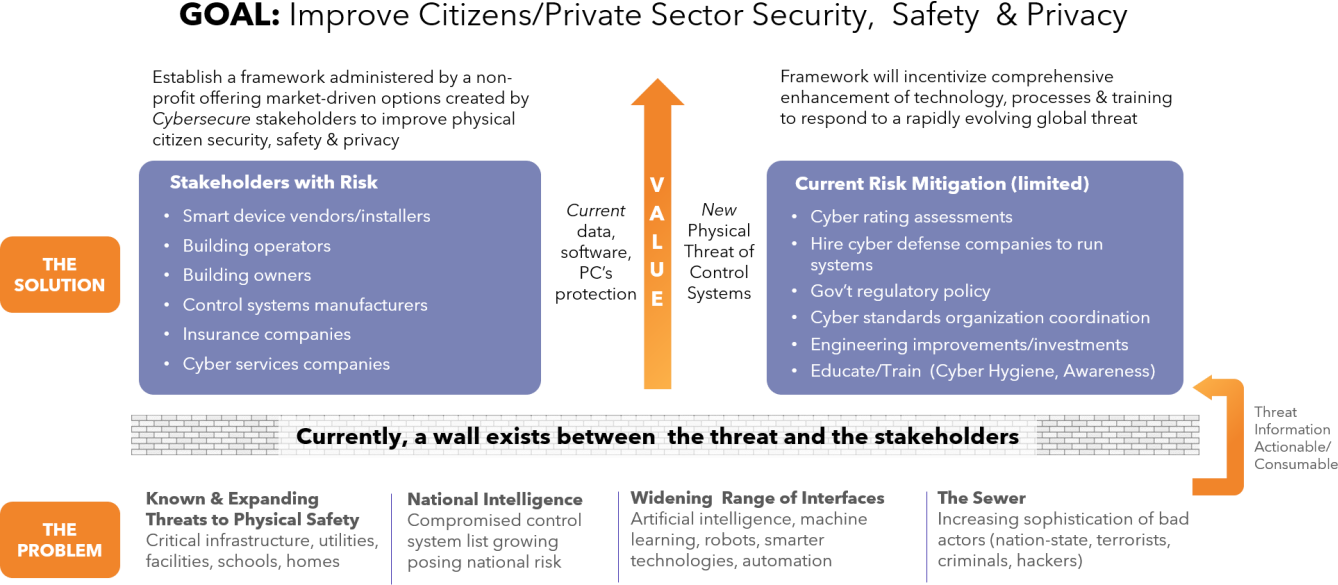


# Anticipated Stakeholders

* Building Owners & Operators
* Critical Infrastructure Operators
* Technology Manufacturers
* Equipment Installers
* Control Systems Manufactures
* Standards Organizations
* Engineering Companies
* Insurance Companies
* Cyber Companies
* Government/Regulatory
* Public Safety Agencies
* Communication Service Providers

# Anticipated Outcome

By simplifying cyber performance risk profile through a rating system and education, this entity can significantly reduce our nation’s threat of cyber attacks. Our overriding goal is to accelerate adoption and use of a newly designed cyber rating program and as a result turn complex threat information into consumable, actionable intelligence.



# Governance Structure and Voting Models

The governance structure of most certification organizations follows a standard model consisting of an Executive Board and a Technical Steering Committee. Cyber security affects all industries, requiring additional subcommittees (Special Interest Groups) focusing on specific industry segment issues.

## Interim Board of Directors – Standing Up Organization

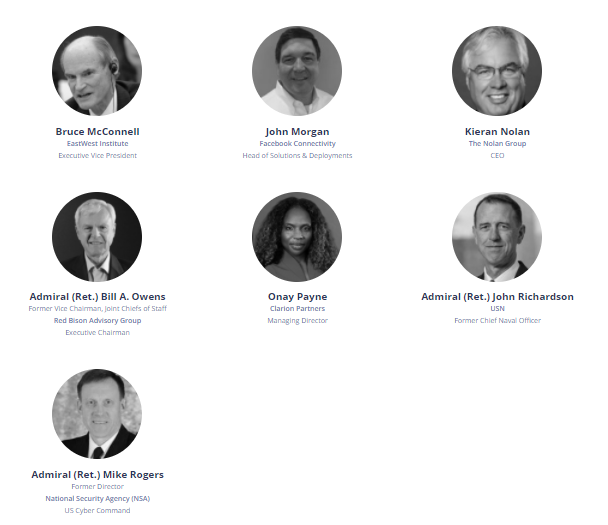
Additional background information on board members can be found at:

https://bcsdev1.wpengine.com/invest/board-of-directors/

**Board of Advisors**

The current Board of Advisors is comprised thought leaders across wide spectrum from the public and private sectors.

**Board of Advisors (continued)**

****

Additional background information on board members can be found at:

**https://bcsdev1.wpengine.com/invest/advisory-board/**

**Size and Composition of Long-Term Executive Board (subject to change)**

The function of the Executive Board is to set the overall strategic direction for the non-profit.

It is critical for the entity and all its stakeholders that this Board performs its functions appropriately and that there is a clear division of responsibilities between the Executive Board, the Technical Steering Committee, and the operational and support staff.

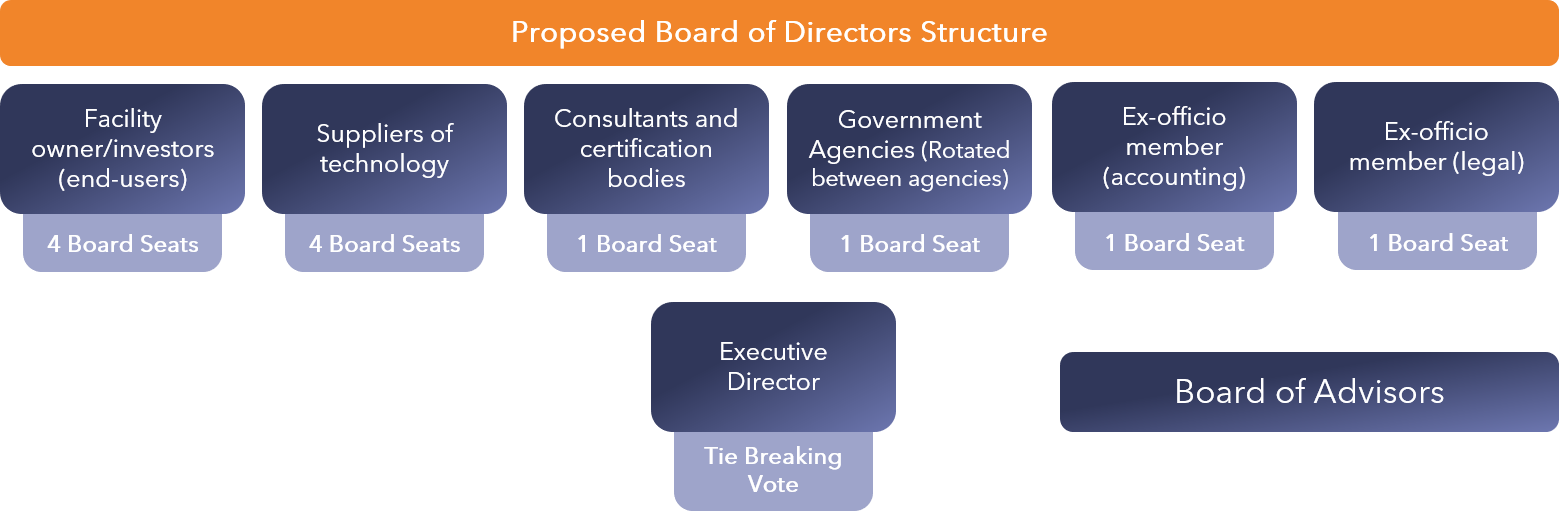
It is important that the Board not become preoccupied with technical issues and rather leave these issues to the Technical Steering Committee and its various sub-groups.

A Board that is balanced by industry sector and member type is essential for maintaining both member- neutrality and industry relevance.

Obviously, a Board that is completely dominated by vendor interests could be an issue, but even sector domination can cause difficulties, unless the consortium has been deliberately established for a specific sector. For example, consider the implications of a Board that contained two individuals from the power utilities, two vendors that only supplied the power sector and two consultants that only serviced the power industry. This would tend to push the organization towards satisfying the needs of the power sector and may neglect the needs of the other sectors. In the end, the organization would lose credibility, which would cause members of the other sectors to seek fulfillment of their needs elsewhere.

At the same time, a balance must be found between representation and workability. The Board must be large enough to provide adequate representation, but it cannot be so large that it becomes a barrier to its own progress. As pointed out in numerous interviews, as Board size increases, it becomes harder to schedule and conduct board meetings.

Since most organizations interviewed felt a board having between 8 to 12 members was ideal, a possible distribution of board seats could be:



In addition, every effort should be made to ensure that the Board is properly balanced in support of the consortium’s mission.

To facilitate decision making, the Executive Director of the entity (Building Cyber Security) should have a vote for tie-breaking purposes, except for matters dealing with his or her performance.

Since the Executive Board should focus on strategic direction and not on technical issues, we recommend that the Board members should be senior management in their respective organizations and not be technically oriented individuals. For example, the Fieldbus Foundation’s board includes people such as John Berra (CEO of Emerson Process Solutions), John Eva, (Vice President and General Manager of Invensys Process Systems) and David Eisner, (Vice President of Engineering of Honeywell).

Members at this management level have the authority to take action on matters resolved during board meetings and do not have to refer back to their companies for all decisions, ensuring that the ENTITY resolutions will not be hampered by management in other organizations, and facilitating prompt action on resolutions.

## Voting

Typically, voting is based on a one vote model for full members and no voting rights for associate members. Founding members may get special voting privileges but this varies.Further, as we noted above, organizations often control the number of seats for each type of member, such as allowing four vendor member seats and four end-user member seats.

Based on these starting points, organizations use one of two voting models for selecting the Executive Board and Technical Steering Committee members. The first is for each member to be able to vote for all seats, regardless of their member type. The second is for each type of member to vote only for the seat reserved for the member of the same type.

## Staffing

Based on the interviews held with successful certification organizations, we strongly recommend that the Executive Director be a professional position. As well, the day-to-day operations should be either contracted-out to a supporting organization or managed by professional staff. Expecting the entity to be largely volunteer-driven is unrealistic.

For example, Andrew Updegrove offers the following advice to companies trying to decide whether to join an established certification organization:

*“While there are examples of all-volunteer consortia that have been quite successful, this type of organization requires greater commitment by both member companies as well as their representatives. If a consortium which lacks paid staff also lacks a culture of strong committee chairs, timely process and continuity of membership, its efforts are vulnerable to failure.”*

In addition, the entity will likely need to engage the services of one of more technical subject matter experts (SME) in the area of security assessments and testing, auditing procedures and, management auditing. While some of this expertise will come from volunteers, we expect that a considerable amount of it will need to be paid for, either through having a professional on staff or through in-kind services from its membership

# Organization/staff org chart



Entity Objectives

* Be managed by an independent, non-profit organization (NPO) with the sole objective of implementing the program to enhance the cyber security of facilities and related infrastructure for the entire ecosystem.
* Identify the standards that apply to specific types of operational technologies (OT) which enable a manager to specify types of physical and cyber CS (Control Systems) protections within an overall risk-management Framework.
* Establish a nationally accredited training program for engineers, technicians and IT managers specifically dedicated to promulgating the standards for OT system security.
* Establish a formal review and certification process of CS designs, specifications, and system installation procedures.
* Identify cyber/physical security measures that can be selected, standardized and rapidly implemented based upon the required security certification tier.
* Provide clear requirements to “smart” manufacturers of the physical, OT, and IT protections

needed to achieve various levels of certification through an independent test facility.

* Assign a nationally recognized CS security rating (about five levels ranging from extremely secure/SCIF to open secure) for each facility/infrastructure and their operations that will be recognized/supported by governments at all levels, industry, consumers, and insurance companies;
* Closely coordinate with federal agencies such as the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) Industrial Control Systems Joint Working Group (ICSJWG) ( https://ics-cert.us-cert.gov/Industrial- Control-Systems-Joint- Working-Group-ICSJWG ), the DHS Cybersecurity and Infrastructure Security Agency (CISA) ( https://[www.dhs.gov/CISA ),](http://www.dhs.gov/CISA)) US CYBERCOM, DOJ Federal Bureau of Investigation, and the National Institute of Standards and Technology (NIST) to disseminate information on the current security threat, provide information to facility managers on compromised systems, and to update security standards.
* Incentivize organizations through a recurring certification process to implement and maintain comprehensive processes and procedures for CS cyber protections, including product registration, maintenance, inspection, penetration/red team testing, event/incident/emergency response, change control/configuration management, and component life cycle management (software updates, sunset products, inventory sparing and identification and testing of suitable substitutes).

# Implementation

The program should be modeled after the successful Leadership in Energy and Environmental Design (LEED) program, which is conducted by the US Green Building Council (information paper attached.

LEED incentivized the architectural/engineering (A/E) community to adopt and include standards for environmentally sustainable facilities. The program matured to the point of a national acceptance of commercial construction standards; and led to the direction by Executive Order for federal agency goals and investments. The program also resulted in the establishment of value for the national A/E industry to voluntarily invest in training to become LEED certified designers, for which they advertised to potential clients.

The International Society of Automation (www.isa.org) is a nonprofit professional association for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops global standards; certifies industry professionals; provides education and training; publishes books and technical articles and provides career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as “The Voice of Automation.” Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium that manages the ISASecure™ conformance certification program. ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against

network attacks and free from known vulnerabilities. ISCI also offers an ISASecure organization process certification for product development organizations. The Security Development Lifecycle Assurance (SDLA) certification promotes security development lifecycle practices intended to improve the quality of security in IAC systems. The ISASecure™ designation is earned by industrial control suppliers for products that demonstrate adherence to industry consensus cyber security specifications for security characteristics and supplier development practices. The ISASecure program is based upon the IAC security lifecycle as defined in ISA/IEC 62443. At this time, the scope of the ISASecure certifications includes assessment of off-the-shelf IAC products and IAC product development security lifecycle practices. ISASecure does not offer assessments for integrator site engineering practices or asset owner operations and maintenance practices. ISASecure certifies off-the-shelf systems; not the site engineered

/ deployed systems. ISCI offers three certifications with four security assurance levels (SAL) in alignment with ISA/IEC 62443.

### ISASecure Embedded Device Security Assurance (EDSA) Certification

1. ISASecure System Security Assurance (SSA) Certification

### ISASecure Security Development Lifecycle Assurance (SDLA) Certification

Other existing implementation models for reference include the Federal Government’s “Energy Star”

program ( https://[www.energystar.gov/](http://www.energystar.gov/) ) promoting the use of energy efficient products, and the

Underwriter’s Laboratory (https://[www.ul.com/aboutul/)](http://www.ul.com/aboutul/)) establishing product and installation safety and health standards.

Building Cyber Security would be established initially by a CS-related trade association.

Eventually, the entity would self-sustain through fees obtained from: 1) professional training certifications; 2) review of designs and installation of the CS architecture; or 3) periodic re- certifications. The NPO would be responsible for a national marketing and awareness campaign to establish the brand and legitimacy of an assigned security rating. This is the only way for customers to be incentivized to invest in periodic reaccreditations. Building Cyber Security would also need to work with the NIST and industry to update the measures required for each level of accreditation as technology and the threat matures.

# Market Analysis

Digital technology and automation have improved efficiency in every facet of business, the government, our military and our personal lives. For facilities and critical infrastructure, Control Systems (CS), often referred to as operational technology (OT) , providing local governance, supervision, and process control to physical systems have been converted from analog to digital platforms using common Information Technology (IT) networks and micro-processors. These highly interconnected and mutually dependent OT devices and networks are vital to the operation of all buildings. While approximately ninety percent (90%) of the nation's critical infrastructures are privately owned and operated, federal agencies also operate these control systems in critical public facilities, Defense infrastructure and other services such as air traffic control and materials handling.

Federal agencies set standards through public-private partnership organizations like the North American Electric Reliability Corporation (NERC) (https://[www.nerc.com/Pages/default.aspx](http://www.nerc.com/Pages/default.aspx) ).

Over the years, well managed certification programs across a broad spectrum of industries have provided clear advantages to their participants. Programs like the TÜV certification for Safety

Instrumented Systems and the Fieldbus Foundation’s device interoperability certificates have had significant positive impact in the industrial control arena, while the USB Implementers Forum’s certification efforts have brought home computer users one of first communications technologies that

operates almost flawlessly, regardless of the product involved. Worldwide, there are tens of thousands of certifications programs across all industries that exist because certification creates tangible benefits for the product user, the product manufacturer, standards bodies and society as a whole.

These benefits can be both tangible and intangible. As noted by not-for-profit’ consortiums that manage

technology certification programs, the typical benefits of certification programs include:

* *Increased probability that the whole (or system or solution) will operate as expected*
* *Improved interoperability of components by assuring common interpretation of specifications*
* *Facilitated improvements in specifications as the process uncovers ambiguities in standards*
* *Facilitated improvements in implementations as the process uncovers ambiguities in products*
* *Accelerated convergence between the specifications and implementations as the process uncovers ambiguities in the specification and errors in interpretationbuilt into products*
* *Improved confidence in deployed technology solutions.*

More specific to the “smart/connected” technology ecosystem, this proposed security certification process/rating will result in significantly reduced costs and time commitment in product selection and acceptance for owner/investors. It will also ensure that products are more secure ‘out of the box’ which, as a result, will offer improved reliability and safety. For suppliers and owner/investors, the certification

process will provide a single assessment framework and an industry stamp of approval, resulting in faster time to market and lower development and integration costs. Finally, for the standards bodies and government agencies developing detailed security specifications, this entity will help translate very technical specifications into to consumable information for the non-cyber expert. The result will be better, field-tested standards that are clearly being followed by industry.

Companies that manufacture these types of systems must understand that cybersecurity is a key aspect throughout the product development lifecycle including support and decommission. Manufacturers need to utilize industry best practices and standards to secure their supply chains, in their operations thereby securing their products, and to minimize cybersecurity threats all along the way.

Based on recent intelligence and government warnings, cybersecurity has emerged as a critical safety and security vulnerability with threats from hostile governments, and terrorist groups to disgruntled employees or anyone with a computer. Control system vulnerabilities can be exploited for data monitoring/theft, service manipulation/disruption/denial or destruction. In extreme cases, controls can be manipulated through a cyberattack to threaten lives and safety. Adding to the concern, smart homes and mobile devices connected to publicly available networks afford bad actors millions more entry points of attack.

While the threats continue to grow, responding policies and programs are disjointed and underfunded. Building owners and operators are not fully aware of the threat and true recovery costs. Investments to enhance protection compete with other priorities based on a probability of occurrence of attack and speculation of impact.

Today, information technology professionals prioritize network protection while building managers prioritize optimal system performance and neither are incentivized or trained to collaborate on protections to control systems.

End-users represent a key stakeholder in responding to the cybersecurity threats associated with increasingly interconnected control systems. End-user education is one of the most under- invested and under-appreciated aspects of cybersecurity. A key component of implementing good cyber hygiene with respect to control systems is obtaining a fundamental knowledge and increased awareness of how to practice it.

Depending on a building’s risk assessment, many standards and best practices can be applied to control

system security, including the National Institute of Standards and Technology (NIST)

Cybersecurity Framework, and the International Electrotechnical Commission/International Society of Automation series of standards on security for industrial automation and control systems (IEC/ISA 62443). It can be challenging assessing which standards apply, based on the degree of risk to their facility or mission.

Responding to increasing risk management demands by end users, third party cybersecurity rating services are providing scores based on industry best practices in order to assess extent of vulnerabilities. Organizations cognizant of poor scores are taking actions to improve for security and reputational reasons. Eventually, cybersecurity ratings may become as important as credit ratings when assessing the risk of existing and new business relationships.

## NATIONAL SECURITY THREATS

Lack of CS (cyber security) around facilities and related infrastructure has emerged as a critical vulnerability. These threats derive from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. CS can be exploited for a wide range of intents, including data monitoring/exfiltration, service manipulation/disruption/denial or asset destruction.

Malwares Stuxnet, Black Energy, and "Crashoverride" manipulates CS in order to damage larger, critical systems. CS has also been specifically exploited for cyberattacks such as ransomware, Distributed Denial of Service attacks, and the distribution of malware to other IT networks.

Russia-originated Dragonfly campaigns initially gained access to the networks of targeted organizations, and then entered a second phase that provided access to operational systems for future disruptive purposes. North Korea’s WannaCry’s attack affected UK’s National Health Service and, in a major threat to the industrial control system market, the Shamoon cyber- attack on Saudi Aramco overwrote the master boot record of thousands of computer hard drives making them unusable. ‘

Network propagation and file-wiping malware NotPetya in 2018, using IT network vectors, caused billion-dollar global physical supply chain impacts into cyber-physical shipping operations. The Black Energy campaign and HAVEX malware attack were specifically designed to exploit CS at the device level; Flame and Duqu malware physically destroyed CS-related IT servers and workstations.

A cyberattack on the Ukraine electric grid in December 2015 demonstrated a sophisticated capability to cut power to mission critical facilities. The CS in Ukraine were more secure than many systems in the US with well-segmented entry points from the control center business networks that had robust firewalls. Attackers avoided these controls because workers logging remotely into the SCADA network that controlled the grid, were not required to use two-factor authentication. This allowed the attackers to

hijack the workers’ credentials and gain access to systems that controlled the electrical substations.

In March 2018, federal agencies issued a Technical Alert on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.

DHS and FBI characterize this activity, called FancyBear, as a multi-stage intrusion campaign by Russian government cyber actors. They targeted the relatively weak cyber defense of small companies and

subcontractor networks where they staged malware, conducted spear phishing, and gained remote access into larger energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to CS.

For the Department of Defense, the 2018 National Defense Strategy articulates its intent to invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Secure and resilient CS are essential to providing warfighting capabilities, executing critical missions, maintaining operational readiness, and projecting power. CS supporting Defense Critical Infrastructure (DCI) are actively threatened and are highly vulnerable to cyber security attacks and failures. Risks to CS increase as more CS devices are connected to networks without appropriate technical cybersecurity protections and strong cyber hygiene practices.

## CHALLENGES

While the threats are documented and growing, the policies and programs for CS protection are disjointed, slow, and underfunded. Investments in cybersecurity measures to protect CS during the design and installation phase, such as firewalls, Distributed Denial of Service (DDOS), behavioral anomaly detection (BAD) tools, encryption, or Database Management System (DBMS) -- as well as operations and maintenance planning to sustain the protection -- are not incentivized and end up competing with other more tangible funding priorities. Developing business cases to enhance protections for legacy systems against a range of possible attacks may be difficult to justify.

Most operational leaders do not believe their systems are under significant threat, nor are they aware of the costs, in lives and dollars, of recovery from an attack.

The lack of understanding of general CS architecture lead managers to believe that these building systems are immune to the threats of IT networks. Upgrading the cyber protection of a CS may require a temporary shutdown of the facility/infrastructure, incurring additional costs or service disruptions.

As a result, the risk of doing something may initially be greater than the risk of doing nothing. In addition, the IT cybersecurity market has grown with a focus on protecting traditional IT devices. The tools often do not work in the CS environment without significant adjustment and tuning. In fact, if improperly installed, they can cause more risk than protection.

The proliferation of smart-city initiatives and investments to enhance the efficiency of public infrastructure and services has also increased the vulnerability of these services to manipulation or exploitation. On a more tactical level, smart home and mobile devices affords adversaries millions of additional entry points to attack infrastructure. Threat actors also could use consumers’ devices to create a bot-net that can carry out large-scale attacks on networks, power grids, or transportation systems.

Smart devices tend to be developed with a focus on features rather than security. The security

responsibility lies with device owner or a company’s IT department. As more connected devices are deployed in enterprise environments—e.g., smart facility management CS — IT security staff may not incorporate CS into security management plans.

The cyber protection of CS is further complicated by gaps in knowledge on adequate design, installation, operations, and monitoring of systems to reduce the risk of exploitation. The critical difference is that IT professionals prioritize the protection of networks and CS technicians prioritize the optimal performance of the CS and the components and devices.

Engineers and contractors selecting a certain CS may not be aware of the cyber risk of CS subcomponents or whether the system has already been compromised. IT security/system admin may not be educated on ways in which malign actors can penetrate CS at the subsystem level to penetrate corporate networks.

CS protection is diverse and scattered throughout the Federal and industrial ecosystems. Depending on risk assessment, there are many standards that can be applied to CS security from NIST and NERC CIP to CSC20 and IEC/ISA 62443. All have their pros and cons, and

organizations get caught in the “paralysis of analysis” when assessing which standards to apply, based on the degree of risk to their facility or mission. NIST establishes security impact levels for Confidentiality, Integrity, and Availability in SP 800-53r4. While these levels are utilized in Risk Management Framework (RMF) for DoD IT, they are not fully leveraged as a means of determining a level of acceptable risk when an asset is being authorized.

In addition, most CS are not Type Authorized that would enable large scale use of Reciprocity across organizations. The Facilities and CIO communities need to collaborate and define what the converged IT- OT CS threats, vulnerabilities, risks, mitigations and operational performance requirements are to ensure the CS and the networks they reside on can fail gracefully and operate even in a degraded safe mode.

Currently, for the prominent manufacturers in the Industrial control system market (ABB Ltd (Switzerland), Schneider Electric (France), Honeywell International Inc (US), Siemens AG (Germany), Rockwell Automation (US), Omron Co (Japan), Emerson Electric Co (US)., General Electric Co (US), Yokogawa Electric Co (Japan), Alstom (France), ISA/IEC 62443 is the current certification process available. (https://isasecure.org/en-US/End-Users/ISASecure-Certified- Devices). NIST and ISA have developed a cross-walk and the joint standards are an example of the vendors, marketplace and standards organizations defining next generation cyber secure products and processes.

# Products/Services

## Membership

Surveys of similar industrial organizations with certification authority indicate that the bulk of the core membership comes from the vendor community, followed by the consulting community.

Typically, end-users are involved in a relatively minor way through structures such as end-user councils. However, if the interest and support shown in the initial “call to action” is any indication, then the membership will come from major equipment vendors, as well as facility owner/investors.

Consultants, certification bodies, public safety organizations, testing houses and academics will likely want to be involved as the NPO evolves.

This would be desirable since they can offer considerable technical expertise. Finally, due to the importance placed on this topic by the US and European governments, we may also see considerable governmental interest. Thus we see these major categories of members:

* Suppliers of “smart” technology
* Commercial Real Estate /Facility owners & operators
* Consultants and certification bodies
* Government/regulatory Agencies
* Associate Members such as industry groups
* Security R&D organizations

This wide variation in member types is good for the entity for a number of reasons. First, it will help prevent the entity from being diverted to meet the needs of special interests, rather than the industry as a whole. Second, it reduces potential for one group to dominate the entity. This wide variation is more likely to provide the range of expertise needed to successfully create the technical solutions that are required to provide for the intended protection. Thus, membership fee structures and policies should be designed to encourage this diversity.

## Assessments: Certification of Building

The entity will review use developed framework to score a building. The integration of each control system into the overall specifications of a building to designate a certain level of safety and protection.

## Annual Recertification

Once a building or device is certified at a certain level, the entity recertify the building based in part on their TPP in responding to evolving threats over the life cycle of the building.

## Longer Term Revenue Opportunities (not reflected in projections)

## Education and Training

The entity will develop a curriculum of study for the protection, design, installation, and operation of control systems which can then be licensed to existing technical training programs both in the IT and the OT ecosystems. The entity will charge for adoption and accreditation of the program. The entity could also accredit each designer or technician.

## Certification Device Design

The entity will review the integration of each control system into the overall specifications of a building or device design to designate a certain level of safety and protection. The entity will also want to follow up with an initial certification of the TTP once a prototype is completed or a building is renovated/constructed/retrofitted.

## Hardware/Technology Certification (Longer term)

The entity will want to partner with existing laboratories and control system manufacturers to identify the specific engineering requirements designed and installed in each control system which would distinguish a tiered standard. This is where control system manufactures will want to pay to play in the development of those characteristics

## Financial Highlights/Projections

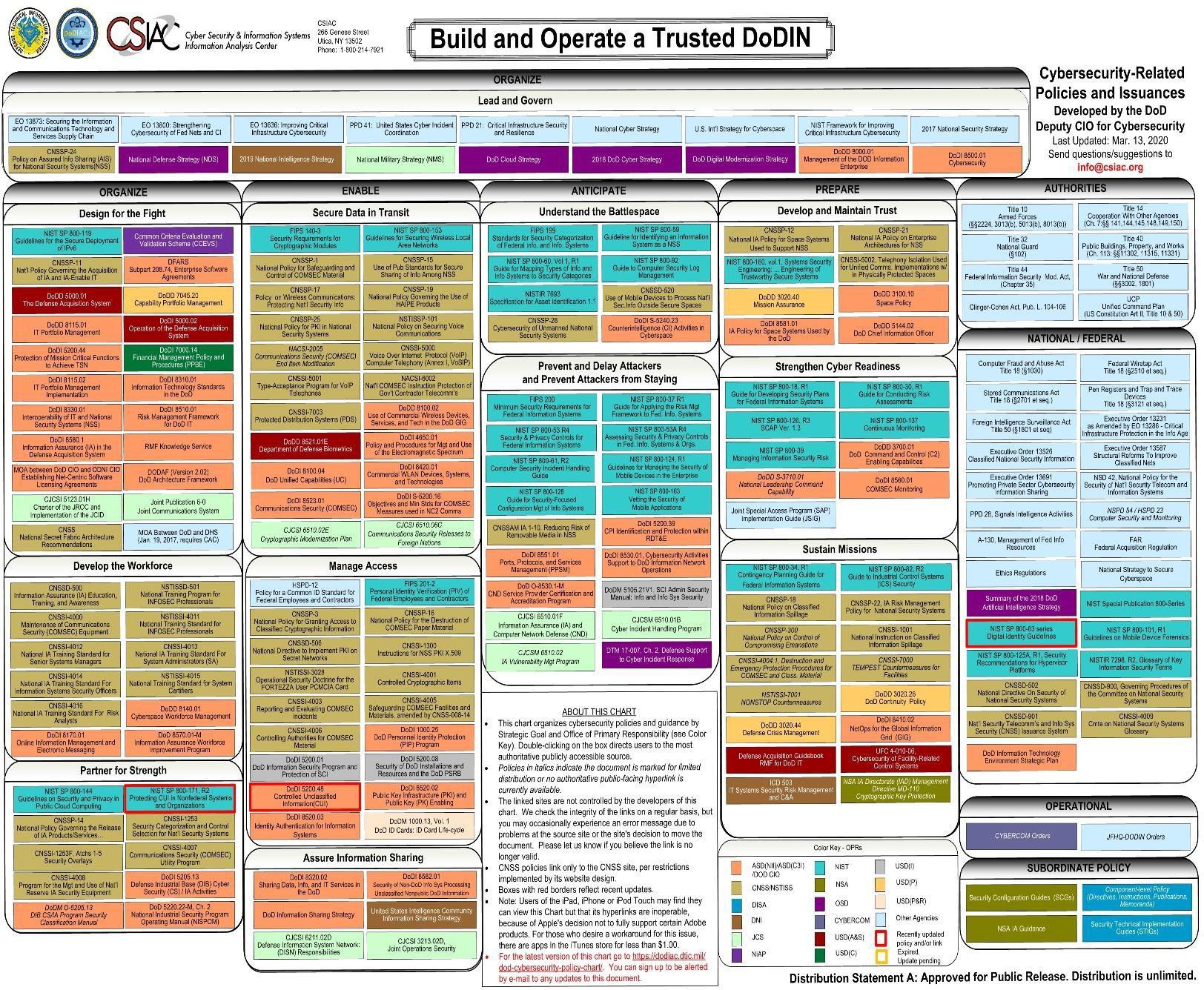


Note Operating Expenses assumes approximately 20 FTE Headcount

# Appendix – Supporting Detail

Current Cyber Security Policies

Complex and not consumable



# Role of Government

In addition to the public policy that would require adoption of our standards, the following opportunities should also be considered

**DHS/CISA -** Control Systems Security are “on the critical list”, but along with a thousand other things, and not being coordinated across the CISA lines at this time. Chris Krebs, Director CISA (https://[www.dhs.gov/person/christopher-c-krebs).](http://www.dhs.gov/person/christopher-c-krebs)) Is likely to recognize the need and may be very willing to have DHS engage in the “support and advise” role.

**Why include the Government? National Level Credibility** – With DHS and Department of Commerce

engaged, the effort becomes the defacto ‘standard’ for the approach. The process both creates a natural barrier to alternative efforts and provides an easy engagement path for stakeholders – “participating in an effort to provide better security” is an easy sell. – Imagine a DHS website that essentially points to your standard and landing page.

**Leveraging an Existing Legal Framework** – The National Instructure Protection Plan (NIPP) and Presidential Policy Directive 21 (PPD21) provide a structure to cooperate, share information, and engagement across critical infrastructure for DHS under CIPAC. The groups that do this are all Critical Instructure Sector working groups (not under DHS, but made up of CI Sector stakeholders.) The three keys here are:

### Provides a legal framework for competitors to effective collude legally.

* 1. Provides a mechanism to coordinate with the government in a non- FOIAable environment (message management).

### Provides a way to engage the stakeholders without having to make them members/board of the NP.

**Federal Government Control** – A key consideration for these efforts is the ‘risk’ associated with another government agency deciding that they should be in charge of this program (NIST, DOC, etc.) With DHS onboard, we can provide a firewall to these organizations, channeling them via DHS.

**Standardization and Implementation –** Lastly, leveraging (A), DHS can be the conduit to the state/local level to promote the standards implementation (under the guise of infrastructure protection.) Downstream government players are much more open to establishing rules and standards that already have national-level backing.

**Proposal to Enhance Control Systems Security by Creating Cross-Disciplinary, National Accreditation/Certification Body**

**BLUF:** Ongoing, expanding cyber threats to Control Systems and the impact of widespread social automation and connectivity requires unified policy and standards. A comprehensive program providing national accreditation/certifications solidifies the United States’ policy and posture, enabling consistent and relevant cyber protection for all critical facilities and

infrastructures. A national program simplifies procedures, driving efficiencies through the entire system.

**NEXT STEPS:** This paper is intended to be distributed as a discussion draft to invite peer review from industry and public partners for concept enhancement, critique, or the identification of challenges and opportunities to moving forward. The goal is for industry or a trade organization to establish a NPO by June 2019 and to publicly release standards by early 2020 due to the urgency of the threat.

**Feedback:** No commercial entity will settle for a less than “platinum” rating if it wants to include the security of its system in marketing materials to separate itself from its competitors. Yet, it may not require, or be able to afford the types of extreme measures needed to rate a nuclear power plant or a hydroelectric dam as “platinum” secure. As a results, the NPO may need to come up with a series of CS standards for critical national infrastructure and hospitals which is different that standards developed for a commercial building, hotel, or data center.

The biggest threat to a rating system is for a building or a CS to be certified at a certain level of security and then to be successfully attacked or exploited. This would undermine the credibility of the system. The accreditation will need to include a caveat that the rating is based on known threats as of the time of the rating.

Should an accreditation include an assessment of the programs in place to protect against an insider attack or the unintentional involvement of third parties?

The NPO will be accrediting training programs provided by others, individuals (designers/technicians/specifiers, installers, and maintainers), buildings or infrastructure, and on-going operations. Each will need to have parameters and conditions for certification.

While public CS security standards exist from various organizations, the CS manufacturing industry should be the lead in proposing the final criteria for accreditation of each level of CS security. The NPO’s first task would be to facilitate the review.

As part of ISA's continued efforts to meet the growing need of industrial control systems professionals and to expand its global leader outreach into the security realm, ISA has developed a knowledge-based certificate recognition program designed to increase awareness of the ANSI/ISA99 standard. This new ISA/IEC 62443 Cybersecurity Fundamentals Specialist certificate program is designed for professionals

involved in IT and control system security roles that need to develop a command of industrial cybersecurity terminology and understanding of the material embedded in the ISA99 standards.

* Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist
* Certificate 2: ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
* Certificate 3: ISA/IEC 62443 Cybersecurity Design Specialist
* Certificate 4: ISA/IEC 62443 Cybersecurity Maintenance Specialist
* ISA/IEC 62443 Cybersecurity Expert: Individuals who achieve Certificates 1, 2, 3, and 4 are designated as ISA/IEC 62443 Cybersecurity Experts.

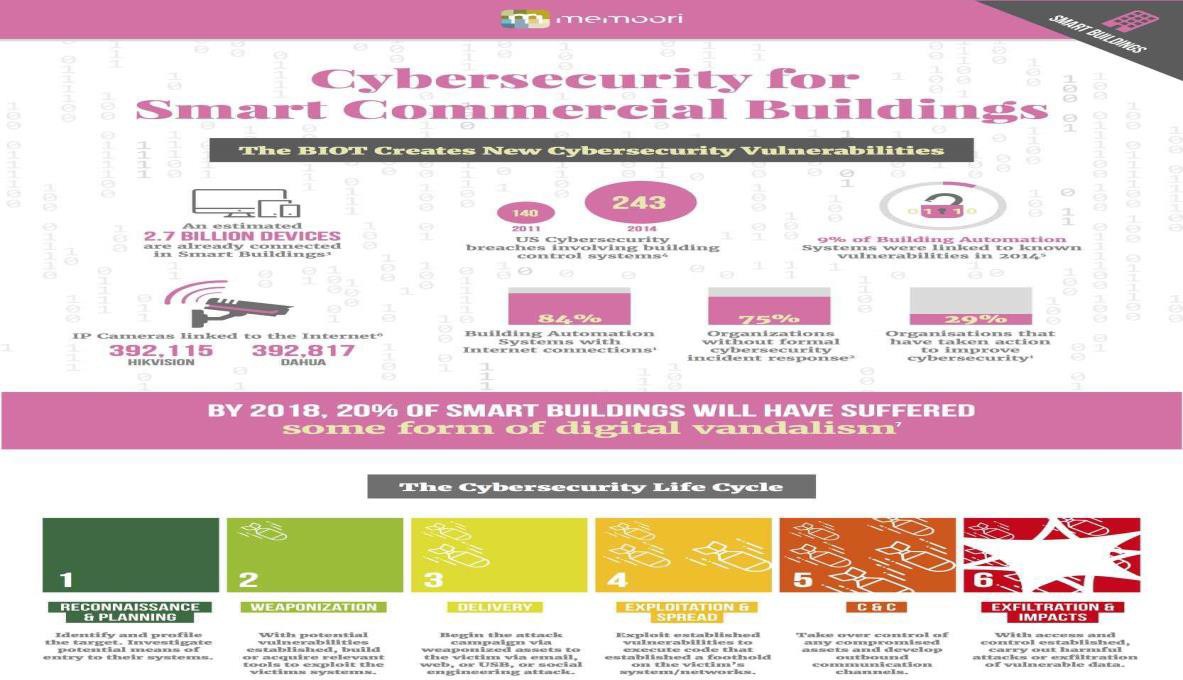
About the ISA Security Compliance Institute (ISCI) Founded in 2007, the ISA Security Compliance

Institute’s mission is to provide the highest level of assurance possible for the cyber security of industrial automation control systems (IACS). The Institute was established by thought leaders from major organizations in the industrial automation controls community seeking to improve the cyber security posture of critical Infrastructure for generations to come. ISCI Members include Chevron, ExxonMobil, Aramco Services, Honeywell, Schneider Electric, Yokogawa, exida,

Codenomicon, CSSC, and IPA-Japan. The Institute’s goals are realized through industry standards compliance programs, education, technical support, and improvements in suppliers’

development processes and users’ life cycle management practices. The ISASecure® designation ensures that IACS products conform to industry consensus cyber security standards such as IEC 62443, providing confidence to users of ISASecure products and systems and creating product differentiation for suppliers conforming to the ISASecure specification. [www.isasecure.org](http://www.isasecure.org/)

# Competitive Offerings

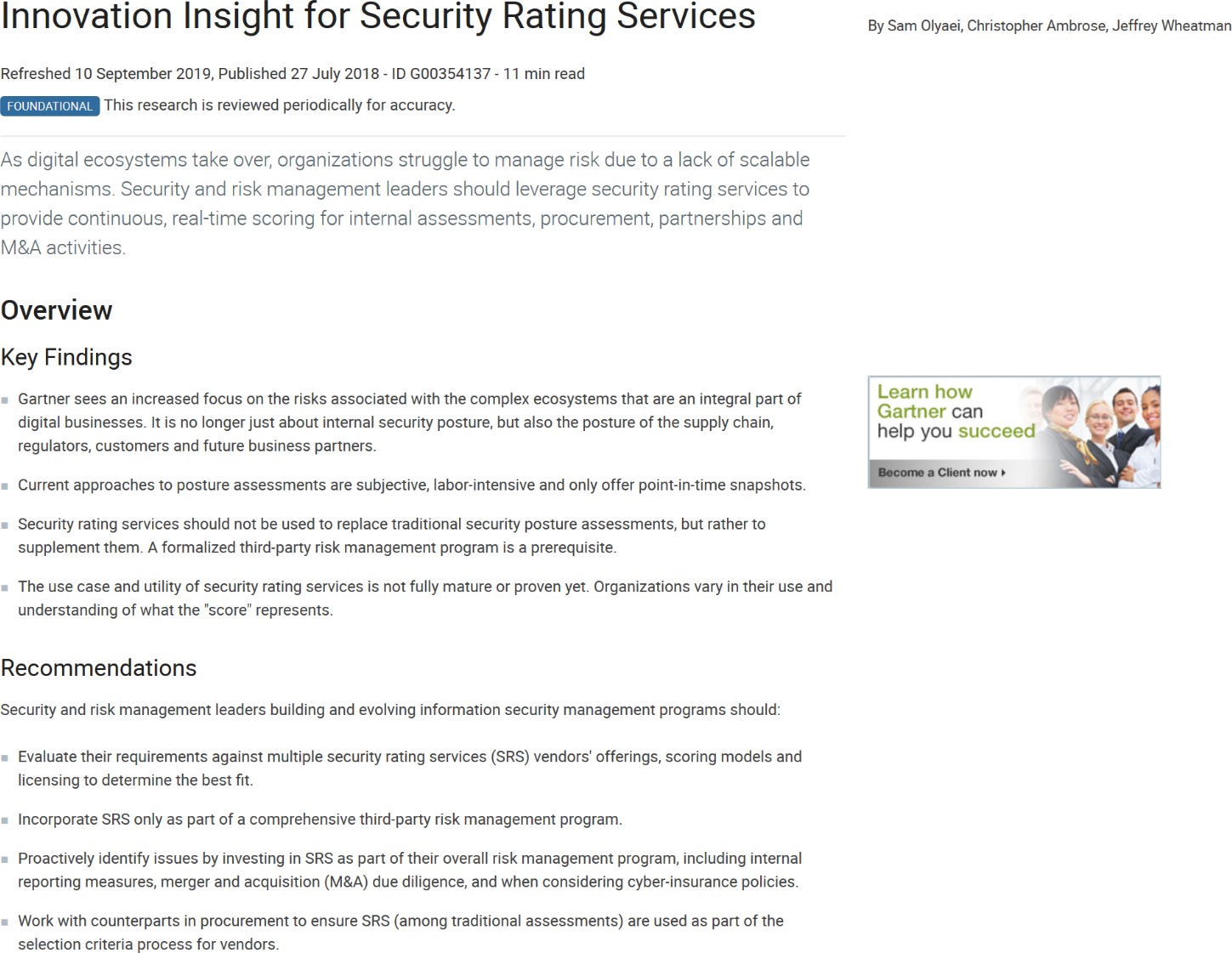








Innovation Insight for Security Rating Services



Click on link below for full report:

[https://www.gartner.com/doc/reprints?id=1-](https://www.gartner.com/doc/reprints?id=1-1OF97ZHD&ct=190826&st=sb&__hssc=127855378.1.1596651878874&__hstc=127855378.87166fc261e24ba3ed1136fec7c2bd81.1596651878873.1596651878873.1596651878873.1&__hsfp=3297900913&hsCtaTracking=3ad53b90-5497-49ea-ab07-b2f5b3ad7c97%7C9a4a0fc5-4fe0-45ae-9c14-38adbf71a8bb)

[1OF97ZHD&ct=190826&st=sb& hssc=127855378.1.1596651878874& hstc=127855378.87166fc261e24ba3ed1136fec7c2bd8](https://www.gartner.com/doc/reprints?id=1-1OF97ZHD&ct=190826&st=sb&__hssc=127855378.1.1596651878874&__hstc=127855378.87166fc261e24ba3ed1136fec7c2bd81.1596651878873.1596651878873.1596651878873.1&__hsfp=3297900913&hsCtaTracking=3ad53b90-5497-49ea-ab07-b2f5b3ad7c97%7C9a4a0fc5-4fe0-45ae-9c14-38adbf71a8bb)

[1.1596651878873.1596651878873.1596651878873.1& hsfp=3297900913&hsCtaTracking=3ad53b90-5497-49ea-ab07-](https://www.gartner.com/doc/reprints?id=1-1OF97ZHD&ct=190826&st=sb&__hssc=127855378.1.1596651878874&__hstc=127855378.87166fc261e24ba3ed1136fec7c2bd81.1596651878873.1596651878873.1596651878873.1&__hsfp=3297900913&hsCtaTracking=3ad53b90-5497-49ea-ab07-b2f5b3ad7c97%7C9a4a0fc5-4fe0-45ae-9c14-38adbf71a8bb)

[b2f5b3ad7c97%7C9a4a0fc5-4fe0-45ae-9c14-38adbf71a8bb](https://www.gartner.com/doc/reprints?id=1-1OF97ZHD&ct=190826&st=sb&__hssc=127855378.1.1596651878874&__hstc=127855378.87166fc261e24ba3ed1136fec7c2bd81.1596651878873.1596651878873.1596651878873.1&__hsfp=3297900913&hsCtaTracking=3ad53b90-5497-49ea-ab07-b2f5b3ad7c97%7C9a4a0fc5-4fe0-45ae-9c14-38adbf71a8bb)