ESTABLISHING A

CYBER SAFETY STANDARD OF CARE

FOR THE BUILT ENVIRONMENT

Framework, Standards Integration, and Roadmap to Professional Licensure

2026 Cyber Safety Summit | National Academy of Sciences, Washington DC | June 10, 2026

Dr. Georgianna Shea, Chief Technologist, FDD CCTI | Lucian Niemeyer, CEO, BuildingCybersecurity.org

This document is the working framework and action plan produced by the 2026 Cyber Safety Summit. It defines the standard, maps who is responsible for what, anchors the framework in existing technical standards, and establishes the specific actions, owners, and deadlines for the next 90 days and beyond.

How to Use This Document

The document serves four distinct audiences. Find your entry point below, then follow the cross-references. Then apply your expertise to answer the question at the end of each section.

If You Are...	Start Here — Then Go To
An Engineer or Design Professional	Part II (definition, scope, and four-layer framework) → Part III (six core requirements) → Part IV (your obligations) → Part V (standards to use now) → Appendix B (standards to obtain)
An Owner or Asset Manager	Part I (why this matters) → Part II (is your facility covered?) → Part III.2 (Technology Registry) → Part IV (your obligations) → Part VI (insurance implications)
An Insurance Professional or Attorney	Part I (the gap and historical analogy) → Part II (the four-layer framework) → Part VI (underwriting requirements and safe harbor) → Part III.6 (handoff package as evidence) → Part VIII (deliverables that produce defensible records)
A Policymaker, Regulator, or Educator	Part I (historical analogy) → Part VII Phases 2–4 (NCEES, curriculum, governance) → Part VIII (17 deliverables) → Part IX (90-day action plan) → Appendix A (working groups)

Part I: The Case for Action

1.1 — The Reason

The Central Gap

When a structural engineer affixes a stamp, the standard of care is well understood. When a fire protection engineer designs a system, accountability for public safety is clear. **But when a digitally connected water treatment plant, transit system, building automation system, or industrial control environment is compromised through a cyber intrusion, there is no recognized engineer of record accountable for ensuring safe operation.**

That cyber safety gap now represents one of the largest unpriced liabilities of aggregate risk in the built environment. The risk is foreseeable, repeatable, and life-safety relevant — yet it remains unassigned within professional engineering responsibility and liability structures.

1.2 — The Historical Pattern

Engineering standards of care have never been created proactively. They have been forged from catastrophe — and they always follow the same sequence: hazard identified, lives lost, profession organized, standard codified, insurance enforced. The question before this Summit is whether cyber safety will follow that pattern reactively, or whether this profession will act first.

Era / Event	Catastrophe	Standard Created
1754 BCE — Hammurabi	Buildings collapsed, killing owners	Builder personal accountability; first construction code
1866 — Hartford Steam Boiler	Boiler explosions killed workers across industrial America	Inspection-based insurance; ASME Boiler Code (1914)
1871 — Great Chicago Fire	300 dead, 17,000 buildings destroyed	Mandatory fire codes; non-combustible construction
1907 — Wyoming PE Licensure	Untrained practitioners caused public harm	First U.S. professional engineering licensure law
1907 — Quebec Bridge Collapse	75 ironworkers killed due to calculation error	PE as public safety guardian; Iron Ring tradition
1950s–70s — E&O Insurance	Design professionals exposed to third-party liability	Errors & Omissions coverage; documentation standards
2021 — Colonial Pipeline Attack	Russian DarkSide seized automated monitoring and billing software connected to valves and meters	Executive orders directing better software standards, revised pipeline standards
Ongoing — Volt Typhoon	Pre-positioned malware in U.S. critical infrastructure	No mandatory engineering response — this Summit acts

Cyber-physical systems present the same conditions that drove every prior standard: **foreseeable hazards, repeatable failure modes, and catastrophic consequences.** The variable is whether the profession acts before the next disaster or after it. **Q1.2 - What major incidents should be added?**

Part II: What the Standard Is — Definition, Scope, and Framework

2.1 — Definition

A Cyber Safety Standard of Care for the Built Environment is the minimum set of professional duties, design practices, technical controls, documentation requirements, commissioning steps, maintenance obligations, and evidence expectations that a reasonable professional must follow when designing, constructing, modifying, operating, or insuring a connected physical system.

It applies when a cyber compromise could reasonably affect: life safety, public health, physical security, building habitability, critical operations, environmental control, emergency response, industrial process safety, continuity of essential services, or significant property or economic loss.

2.2 — Operational Technology Systems Covered

System Category	Examples
Building Automation for all commercial facilities	HVAC controls, building management systems, energy management, lighting control, smart building platforms
Life Safety Interfaces	Fire alarm monitoring, emergency response, mass notification — where networked connections exist
Access and Security	Physical access control, video surveillance, perimeter monitoring
Vertical Transportation	Elevators and escalators with firmware-based controls or remote access
Utilities and Energy	Power generation, transmission, microgrids, distributed energy, backup power, water/wastewater SCADA, utility distribution controls
Telecommunications	Phones, broadband infrastructure, routers, satellites, GPS/PNT devices
Medical Equipment/Devices	Hospital controls, laboratory automation, environmental control for sterile areas, medical devices, robots,
Industrial Control Systems	Manufacturing, process control, chemical, oil and gas, and other OT-heavy environments with connected communication
Transportation Infrastructure	Ports, airports, rail, logistics automation, runway lighting and control
Transportation Systems	Aircraft, automobiles/trucks, unmanned systems, pipelines, space delivery, material handling/cranes

Q2.2 - What additional systems should be covered?

Devices/ Robotics	Connected Autonomous systems, appliances, sentient beings
Digital and AI-Enabled Systems	Digital twins, AI-enabled optimization, autonomous/semi-autonomous control platforms, IoT networks
Remote Access Systems	All vendor-managed, owner-managed, or integrator-managed remote access to any of the above

2.3 — The Four-Layer Framework

The standard operates in four integrated layers — the same structure that governs fire codes, structural standards, and electrical codes.

Layer	What It Contains
Layer 1 — Legal and Code Baseline	Compliance with applicable law, building codes, fire codes, electrical codes, safety codes, sector-specific regulations, and authority having jurisdiction requirements. Establishes the legal floor — but cyber safety risk routinely falls between existing codes, which is why this standard is needed.
Layer 2 — Consensus Standards	Recognized standards translated into engineering duties: DOE Cyber-Informed Engineering Strategy (2022); ANSI/ISA-62443-2-1-2024 (updated January 2025); NIST SP 800-82 Rev. 3 (September 2023); ASHRAE Guideline 13-2024 (including new Chapter 9 on cybersecurity); NCEES PE Control Systems CBT Section 2.D. Critical Infrastructure Sector standards developed by industry. (ie Critical Infrastructure Standards for utilities, BuildingCyberSecurity (BCS) Standards for commercial facilities, AWWA standards for water systems. The standard translates these frameworks into specific design, construction, and operational obligations — it does not merely cite them.
Layer 3 — Professional Practice	The duty of reasonable care. Competent professionals must: identify connected systems, evaluate consequences, specify controls appropriate to the consequence class, document residual risk, verify installation, commission protective functions, and hand over documentation to the owner.
Layer 4 — Insurance and Liability	The enforcement mechanism. Insurers use the standard to determine underwriting requirements, premium structure, exclusions, and claim defensibility. Documented compliance reduces professional liability exposure. Failure to address foreseeable cyber-physical risk constitutes a defensible negligence argument.

Q2.3 - What edits or additions would you make to this framework?

Part III: What the Standard Requires — The Six Core Elements

These six elements are the operational core. Together they constitute the minimum standard of professional practice for any covered project. Use them directly in contracts, specifications, and project documents.

3.1 — Consequence Classification (Required on Every Covered Project)

Assign a consequence class at project initiation based on what could happen for occupant or user life, safety, or health if a connected system is compromised — not data sensitivity. The class drives every subsequent requirement.

Class	Definition and Examples — Higher Class = Stricter Requirements
Class 1 — Low Consequence	Compromise causes inconvenience or minor disruption. Example: lobby display, non-critical lighting in a non-life-safety area. Basic screening only required.
Class 2 — Operational Consequence	Compromise disrupts system operations or service delivery. Example: commercial HVAC in an office building with no life-safety dependency. Full Technology Registry and minimum design controls required.
Class 3 — Safety or Security Consequence	Compromise could affect life safety, health, physical security, emergency response, or occupant protection. Example: hospital HVAC in surgical suites, water treatment SCADA, school access control. All Class 2 requirements plus technical cyber commissioning verification.
Class 4 — Critical Infrastructure or Mission Consequence	Compromise could affect essential services, national security, public health, or industrial process safety. Example: power grid control, airport runway systems, major water utility, military installation. All Class 3 requirements plus continuous monitoring, independent validation, and recovery exercises.

Q3.1 – What additional details should we add to determine consequences?

3.2 — Technology Registry (Required Class 2 and Above)

Initiate at project conception within a digital twin or database. Maintain through full lifecycle. Includes the technologies imbedded in the project systems and planned to be introduced by the owner. The registry is the foundational document maintained by a Technologist of Record during the design/construction phase and passed on to the owner's engineers and operators after completed construction to be updated and used during the life cycle sustainment/maintenance phase — every other requirement refers back to it.

Registry Field	Why It Matters
System name and owner	Establishes accountability from day one
Designer/specifier; installer/integrator	Documents the professional chain of responsibility

Vendor; product support status; maintenance schedule,end-of-life date	Life cycle maintenance schedule facilitates planning for predictive/preventative maintenance, planned obsolescence, Flags unsupported components — a primary attack vector; must have risk treatment plan
Network connection; remote access method	Maps every pathway available to an attacker
Cloud and wireless dependencies	Identifies externally-hosted risk surfaces outside direct owner control
Physical process controlled	Connects the digital system to its physical consequence — drives class assignment
Authentication method; logging capability	Establishes baseline protection documentation for commissioning and insurance
Patch/update responsibility; maintenance contract owner	Assigns lifecycle obligations to named parties
Commissioning requirement; incident response contact	Links to handoff and response obligations
Consequence of failure or exploitation	Maps impacts to other systems and assists with prioritization
Residual risk decision owner (signed)	Records who accepted what risk, in writing — essential for claim defensibility

Q3.2 – What additional fields or information should be captured in a technology registry?

3.3 — Minimum Design Requirements (Required Class 2 and Above)

The Engineer of Record must be educated and trained in current digital threats and conditions to determine the risks and consequences of Class 2 and Above incidents. The engineer must then make deliberate and proactive decisions to design the following control domains and to specify unique systems, technologies, platforms, or technologies for the protection of systems that can meet the requirements of a Standard of Care to mitigate life, safety, health, and system operations risk.

Control Domain	Minimum Specification Requirement
Network Segmentation	Allow for Isolation of life-safety OT networks from IT, guest, and internet-facing systems. No shared credentials or pathways between operational and administrative networks. Separate safety-critical functions from non-essential functions.
Authentication and Access Control	Eliminate all default credentials before commissioning. Multi-factor authentication for remote access. Role-based access control. Documented vendor access management with approval and logging.
Monitoring	OT-capable tools (not standard IT SIEM) detecting anomalies in industrial protocols (Modbus, BACnet, DNP3). Baseline and deviation alerting. Time-synchronized logs retained minimum 90 days.

Resilience and Recovery	Cyber incident response plan coordinated with operations staff. Backup/recovery for control system configurations. Manual override and safe-mode for Class 3–4 life-safety systems. Documented fail-safe behavior.
Vendor and Supply Chain	Vendor must disclose: remote access requirements, patch procedures, vulnerability notification process, software/firmware inventory, end-of-life dates. Contractual security obligations required.
Exploitation/Incident Reporting	Warn of data/power or other anomaly indicating a cyber incidents with physical consequences that could threaten human safety. Report parallel to occupational safety or structural failure reporting. Post-incident review required for Class 3–4.

Q3.3 – Is isolation the preferred method of network segmentation? What other design requirements should be mandatory for Class 2 and above?

3.4 — Contract and Specification Integration

Mandatory Cyber Safety requirements must be written into project documents at inception — not retrofitted after procurement. The specifications must include instructions to the builder to install technologies, platforms, and applications that offer capabilities identified in Section 3.3 for the protection of Level 2 or above of registry items in 3.2 to mitigate risk in known cyber threats. The builder must be accountable that products selected for installation meet the specifications, and are correctly installed and operating per vendor specifications. The effective operation and sustainment of these requirements must be carried forward into the life cycle operation of the project. Required in:

Document	Required Cyber Safety Content
Owner Project Requirements (OPR)	Consequence class assignment; Technology Registry initiation requirement; Cyber Safety EOR designation for mandatory protections
Division 01 — General Requirements	Cyber Safety Engineer of Record scope; coordination obligations; Instructions for vendor and system submittal process to cyber security engineering for review, cyber commissioning requirements
Division 25 — Integrated Automation	Full cyber safety specifications; segmentation requirements; installed cyber safety applications and technologies, credential management; commissioning acceptance
Mechanical / Electrical / Fire / Security Specs	Cyber safety requirements at each system-specific discipline interface
Vendor and Integrator Contracts	Security disclosure; default credential removal; patch obligations; commissioning participation; insurance requirements
O&M Contracts	Maintenance obligations; annual access review; recertification schedule; incident response obligations

Q3.4 – Where else in the project documents should cyber safety be addressed? What other items should be included as mandatory safety specifications?

3.5 — Cyber Commissioning

Commissioning verifies the as-built system matches the Technology Registry and all design intent. It is a condition of project acceptance — not a post-occupancy option. This commissioning should be accomplished by an independent assessor on behalf of the owner during the construction phase as systems are installed.

- Installed system matches approved Technology Registry and submittal documents
- Network segmentation verified; no unauthorized pathways present
- All default credentials changed; administrative accounts documented
- Remote access controlled, approved, and logging confirmed
- Backups tested; recovery procedures demonstrated
- Fail-safe and manual override modes demonstrated for life-safety systems (Class 3–4)
- Owner personnel trained; training records documented
- Residual risks documented and signed off by owner
- Full Cyber Safety Handoff Package delivered (see below)

Q3.5 – Do we need a standardized Scope of Work or specification for a cyber-commissioning process? What other items should be included in the SOW?

3.6 — Owner Handoff Package and Standard of Care

A project is not complete until the owner receives the Cyber Safety Handoff Package — the cyber equivalent of as-built drawings and fire alarm records, preferably within the development of a virtual or digital twin of the completed project. The package must include:

- Final Technology Registry (as-installed version)
- Network diagrams and system architecture documentation
- Base-line performance data on installed, connected systems (power, data, air, water, fire suppression agent) than can offer a digital twin metrics to determine anomolies
- Account and access management procedures
- Instructions and liability determinations for all third party service providers
- Occupant instructions, roles, and responsibilities
- Vendor access list; remote access procedures; approval process
- Patch and update responsibility matrix with named owners
- Backup and recovery procedures with test results
- Incident response - occupant warnings, contacts, and escalation procedures, drills and exercises
- Training records for all owner personnel
- Commissioning results; deficiency correction records
- Residual risk acceptance documentation (signed by owner)
- Insurance-relevant documentation package

After handoff, the owner assumes accountability/liability for safety, and is responsible for the training of system operators, adequate operation of all systems, maintenance, patching, upgrades, modernization, continuous monitoring/commissioning, annual safety recertification, and safety threat awareness. This includes review of technology registry, remote access, and vendor accounts; verify backups and monitoring are functional; update risk acceptance for

unresolved deficiencies; require risk treatment plan for any unsupported or end-of-life components.

Q3.6 – How should owner requirements be formally developed consistent with a Cyber Safey Standard of Care? How can insurers require compliance during the life cycle of the asset?

Part IV: Assigning Responsibility and Liability

The standard distributes accountability across every party that touches connected physical systems. Engineers who fail to either implement mandatory safety controls or specify additional controls based on the classes in 3.1. Constructors (installers and integrators) who fail to comply with the design and specifications. Owners who fail to maintain safety system or disclose safety threats. Vendors who fail to provide safe products or secure their performance. All carry proportionate responsibility to maintain awareness of changing threats and to proactively respond with effective measures to protect human life, safety, health, and property.

Party	Core Obligations	Key Accountability Trigger
4.1 Cyber Safety Engineer of Record	Identify connected systems; assign consequence class; Specify both mandatory and adequate controls; develop Technology Registry; Specify cyber protection technologies and occupant/user protections; Review and approve product submittals; Require cyber commissioning and review findings; Provide handoff package for cyber safety; Document residual risk. Maintain professional development throughout career on emerging cyber threats and technologies	Professional liability attaches when foreseeable cyber-physical risk was not addressed in design
4.2 Traditional Engineers of Record	Coordinate with Cyber Safety EOR at discipline interfaces; document assumptions and exclusions in writing; Coordinate product submittal reviews and connected system configuration instructions, Coordinate system patch and maintenance requirements; Identify owner-furnished systems that affect safety	E&O exposure when cyber-physical risk crosses into their discipline scope without coordination
4.3 Owners and Asset Managers	Disclose all connected technologies; assign named responsible personnel (IT, OT, facilities, security, incident response); accept or reject residual risks in writing; Implement industry recommended cyber hygiene practices for employees and occupants; Maintain all items in Part 3.6; Maintain persistent training and threat awareness/assessment related to occupant/user safety; Notify insurer of material changes.	Owner liability for operational decisions after handoff, regardless of attack source
4.4 Vendors and Technology Integrators	Obtain Cyber Secure designation; Remove default credentials; disclose remote access requirements; provide firmware inventory and end-of-life dates; carry appropriate insurance; participate in commissioning; resolve deficiencies before acceptance	Technology E&O and contractual breach when security obligations not met
4.5 Professional Societies and Regulators	Adopt standard; engage NCEES on PE exam; engage ABET on curriculum; develop model law for licensure; support safe harbor for compliant practice; Establish a separate society for Cyber Safety Engineering to engage with public policy makers, standards organizations, and insurers; Establish professional development/education standards and certifications for Cyber Safety engineers; Coordinate with insurers to recognize and require Cyber	Institutional duty to recognize cyber safety as a public safety engineering obligation

	Safety Standards of Care in liability, property, and casualty coverage.	
4.6 States	Develop and implement professional engineer licensing requirements for Cyber Safety Engineering to practice as a designer of record.	Responsibility to the public to implement requirements for safety in engineering
4.7 Insurers	Develop formal assessment and compliance guidance for all liability, cyber, property, and casualty policies to mandate certain human safety controls and mitigate cyber risk.	Not all aggregate human safety risk can be transferred and assumed by insurers.

Q4 – What other roles, responsibilities and liabilities should be assigned? What guidance should be developed to determine whether cyber safety risk is assumed, transferred, or mitigated?

Part V: Standards Integration — What to Do With Each Standard Now

These standards form the technical backbone of the Cyber Safety Standard of Care. The table below specifies the immediate action required with each standard — not just its relevance.

Standard	Current Status	Immediate Action Required
5.1 - ANSI/ISA-62443-2-1-2024	Published January 2025. UN-endorsed. Covers building automation, power, medical, transportation, process industries. Four security levels (SL 1–4); shared responsibility model for owners, integrators, and suppliers.	Map ISA SL 1–4 directly to Consequence Classes 1–4. Use Part 2-1 asset owner program requirements to inform Section 6.2 owner obligations. Engage ISA99 Committee for built-environment-specific guidance. Contact: isa.org/standards
5.2 - NIST SP 800-82 Rev. 3	Published September 2023. Expanded scope to full OT. Consequence-based risk categorization separating availability from confidentiality/integrity. OT-specific guidance for 800-53 Rev. 5 control families.	Use consequence-based categorization to validate Class 1–4 assignments. Apply OT incident response guidance (safe operation priority over IT isolation) to Class 3–4 response obligations. Request NCCoE built-environment implementation guide — 2027 target. Contact: csrc.nist.gov
5.3 - DOE CIE Strategy + INL Implementation Guide	Strategy released June 2022; INL Implementation Guide August 2023. Five pillars. 12 engineering principles. 200-member Community of Practice. Consequence-focused design principle is core.	Use INL CIE Implementation Guide as lifecycle application framework. Engage Ben Lampe (Benjamin.Lampe@inl.gov) to incorporate CIE curriculum into WG2 academic framework. INL curriculum is the foundational academic resource.
5.4 - ASHRAE Guideline 13-2024	Published July 2024. Full cybersecurity chapter added (Chapter 9). Covers BAS network design, security requirements, contractor roles. The current standard for BAS specification.	This is the closest existing precedent. Advocate via ASHRAE TC 1.5 to make Chapter 9 requirements mandatory (not advisory) and tied to consequence class. WG1 lead: engage ASHRAE by September 2026.
5.5 - NCEES PE Control Systems CBT	October 2022 specifications. Section 2.D already covers security lifecycle, risk assessment, access controls, and verification of security levels. 85 questions; 9.5-hour exam; once per year (next: April 2027). 232 first-time candidates; 62% pass rate.	Submit proposed additions to Section 2.D by October 2026 (see Phase 2 roadmap): consequence classification, Technology Registry, cyber commissioning, OT incident response, professional duty documentation. Contact NCEES: ncees.org/exams/pe-exam/control-systems/
5.6 - ABET Engineering Accreditation	2025–2026 EAC criteria already require cybersecurity engineering programs to address: OT security requirements; analysis/design/protection of systems with hardware, software, and human components. GMU BS program (2015) is the reference	Petition ABET EAC for program criteria specifically addressing cyber-physical systems in the built environment. WG2 lead. Engage Prof. Peggy Brouse (prouse@gmu.edu) as primary curriculum advisor. Target: ABET petition filed by mid-2027.

	model — hundreds of graduates annually.	
5.7 - Need to add Industry Standards	CIS, MITRE, BCS, AWWA	
5.8 - Need to add cyber engineer Professional Development Standards	Specific certifications and annual requirements for continuing education credits	
5.9 - Need to add Insurance Standards		
5.10 - Federal Standards for certain critical infrastructure sectors	CIP, pipeline, aviation	
5.11 - Integration of Global cyber safety policies and standards		

Q5 – What other standards should be identified and what is their current status? What other actions should be assigned? Do you want to assume leadership for a specific action?

Part VI: Insurance and Liability — The Enforcement Mechanism

The Insurance industry has a critical role in determining which engineering standards and controls must be mandatory to mitigate risk to human life, health, safety, and property. Insurers do not need to become engineering regulators. They need documented evidence that reasonable cyber safety practice are being followed in the design, construction, and operation of an asset.

6.1 — What Insurers Should Require

Minimum questions for underwriting property, professional liability, and cyber coverage for risk in the built environment impacting human safety:

Underwriting Question	Standard of Care Element Tested
Has a cyber-physical consequence class (1–4) been assigned?	Foundation of the standard — drives all other requirements
Is there a current Technology Registry?	Core documentation; absence signals no standard of care was applied; Does the registry include owner-installed equipment?
Were cyber safety requirements in design and procurement documents?	Division 01/25 integration — was it designed in or added after?
Was a Cyber Safety Engineer of Record designated?	Professional accountability — who signed off?
Were connected systems commissioned for cyber safety?	Verification that design intent was actually implemented
Are remote access paths documented and controlled?	A leading cause of OT incidents — vendor and contractor access
Is a penetration testing program in place?	Is the owner receiving constant feedback on vulnerabilities
Are logs enabled and retained for minimum 90 days?	Detection and forensic capability
Are backups tested and recovery procedures documented?	Resilience — can operations be restored after compromise?
Has the owner received a Cyber Safety Handoff Package?	Establishes owner obligations post-handoff; reduces engineer ongoing liability
Are residual risks documented and signed by the owner?	Critical for claim defensibility — what was accepted, by whom, when

Do asset owners and operators have an established program to maintain awareness of emerging cyber threats?	Enforces the owner responsibility for occupant or asset operator safety
Are asset operators trained to maintain cyber protection systems, to implement industry-recommended cyber hygiene practices, and to diagnose and respond to a cyber incident?	Enforcement of password strength, Multi-Factor Authentication (MFA): Active monitoring and management of all connected devices to quickly determine a life threatening exploitation.
What are the programs and budgets for life cycle maintenance and continuous cyber commissioning?	Lifecycle and security patch maintenance — cyber safety degrades without active management
What are the cyber incident response plans? How are incidents reported and post-incident reviews completed?	Priority for preservation of human life, health, safety, and property. Pattern detection; demonstrates active risk management culture
What are the anticipated business disruption costs?	Owner acknowledgment of the financial consequences of a cyber attack to the asset

Q6.1 – Should insurers develop a standard set of requirements and actions to mitigate safety risk? What safety controls must insurers include in policies? Are periodic audits effective or should an insurer require continuous confirmation of compliance with policy requirements?

6.2 — Safe Harbor and Liability Consequences

Organizations That Follow the Standard	Organizations That Do Not
Stronger E&O claim defensibility	Higher premiums; potential policy exclusions
Premium credit potential for documented cyber-safe design	Increased professional liability for foreseeable unaddressed risk
Clear safe harbor when reasonable care is documented	Contractual noncompliance; negligence arguments in litigation
More defensible procurement and owner acceptance records	Required remediation as condition of coverage renewal
Insurance market recognition of risk reduction	Reduced claim defensibility in cyber-physical loss events

Q6.2 – What other incentives can insurers provide to engineering companies to add a licensed Cyber Safety engineer as a designer of record?

6.3 — Insurance Product Alignment

Each product type should incorporate the cyber safety standard as follows:

- **Professional Liability / E&O:** Underwriters must ensure that engineering firms and cyber safety engineers understand the risk to their license, and practice in accordance with the cyber safety standards and professional development requirements; Cyber-physical design failures must be explicitly covered or explicitly excluded — not left ambiguous in policy language
- **Property and Casualty:** Reference the standard in underwriting questionnaires and price responses accordingly; Require mandatory cyber safety controls and consequence classification at renewal
- **Builders Risk:** require cyber commissioning completion before project acceptance — equivalent to certificate of occupancy
- **Cyber Insurance:** Determine whether the facility was designed with cyber safety standard; price risk accordingly and offer incentives for positive performance, including penetration testing, continuous monitoring, and updated protections to respond to emerging threats.
- **Technology E&O (vendors/integrators)**: require commissioning participation and compliance with vendor obligations in Section IV
- **OCIPs/CCIPs**: incorporate Technology Registry as a required schedule to the program

Q6.2 – How else can underwriters drive the incorporation of mandatory cyber safety controls into a project?

Part VII: The Roadmap — Seven Phases to Establish the Standard

Each phase builds on the previous. Phases 1–2 must begin today. Phases 3–5 run in parallel through 2028. Phases 6–7 are the long-term institutionalization targets. **All names are proposed and do not represent commitments unless positively verified in writing. The named have not been contacted to verify interest.**

Phase 1

Convene and Declare — Summit Deliverables

June 10, 2026 (Today)

Action Required Today	Owner
7.1a - Adopt the Summit Declaration: cyber safety is a life-safety engineering responsibility within the professional standard of care	All Summit participants — vote before close of plenary
7.1b - Confirm Cyber Safety Engineer of Record definition: scope, four duties, liability framework, consequence classification	Panel 5 lead — Lucian Niemeyer
7.1c - Confirm WG1, WG2, WG3 chairs; distribute charters and 90-day deliverable commitments (see Appendix A)	Lucian Niemeyer — by end of Summit
7.1d - Adopt the 17 deliverables list (Part VIII) as the working group output mandate	WG chairs — confirmed at Summit
7.1e - Formally request written governance commitment from ISA, ASCE, and IEEE representatives present	Lucian Niemeyer — by end of Summit
7.1f - Confirm the NCEES submission owner for the October 2026 deadline	WG1 Chair — confirmed at Summit

Q7.1 – Are any additional actions required, or do the proposed actions need to be amended?

Phase 2

Anchor in the Examination — NCEES Submission

July–October 2026

7.2- The highest-leverage near-term action. The NCEES PE Control Systems exam already contains Section 2.D on security — the Summit can proposes specific additions, or agree to develop an entirely new exam for cyber safety engineers.

What Section 2.D Already Contains (Existing Exam Content)

Security (physical, cyber, network, firewalls, segregation, access controls); security lifecycle (assessment, controls, audit, management of change); security management system requirements; security risk assessment and system design; verification of security levels (Level 1, Level 2).

This is the foundation. The Summit proposes the additions below to complete it, or to write an new PE exam for cyber safety engineering.

7.2a - Proposed Additions to Section 2.D

- Consequence-based classification methodology for connected physical systems (Class 1–4)
- Technology Registry: development, maintenance, and documentation as a required engineering deliverable
- An understanding of the interactions in 2.2 of this plan
- Proficiency in the items in 3.3 of this plan
- Cyber commissioning: scope, verification methods, and acceptance criteria
- OT-specific incident response: prioritize safe operation over IT isolation protocols
- Professional duty documentation: residual risk acceptance, owner handoff, recertification obligations
- ISA/IEC 62443 security levels mapped to physical consequence assessment
- Knowledge of other industry frameworks and innovative technologies

Q7.2a – What other fields of proficiency need to be included in a PE exam to address cyber safety?

Action	Owner — Deadline
Contact NCEES committee staff re: next exam revision cycle	Building Cyber Security — July 10, 2026
Draft proposed Section 2.D additions	WG1 (Ben Lampe, David Brearley) — August 31, 2026
Circulate draft to all Summit technical panelists for review	WG1 Chair — September 15, 2026
Submit formal proposal to NCEES	Building Cyber Security + FDD — October 2026
NCEES follow-up and inclusion timeline confirmation	Designated liaison — Quarterly from November 2026

Q7.2b – Do we propose amending the Control System PE exam or establishing a new PE exam for cyber safety engineering? Or do we do both?

Phase 3

Build the Academic Foundation — Curriculum

2026–2028

7.3 - George Mason University's BS in Cyber Security Engineering (founded 2015, own department since 2021, hundreds of graduates annually) is the reference model. Other Universities have developed similar programs and are encouraged to participate establishing core requirements for a cyber engineer. ABET EAC already accredits cybersecurity engineering programs. The path exists — extend it to cyber-physical systems in the built environment and reward 4 year graduates in cyber engineering with a path to a professional licensure.

Course Area	Core Content	Primary Resource
Cyber-Physical Systems Fundamentals	IT/OT convergence, SCADA/ICS/BAS architecture, attack surfaces, ISA 62443 foundational requirements	INL CIE Program; ISA/IEC 62443; NIST SP 800-82r3
Threat Intelligence and Consequence Analysis	Threat actor TTPs, CIE consequence-focused design, Volt Typhoon case studies, physical consequence modeling	FDD CCTI; CISA; INL CIE Implementation Guide (Aug 2023)
OT Security Engineering and Specification	Network segmentation design, authentication, monitoring tools, ASHRAE Guideline 13-2024 Chapter 9	UTSI (Shaun Six); Dragos; Forescout; Johnson Controls; Chinook
Technology Registry and Standards Practice	Consequence classification, registry development, Div 01/25 specification, ISA 62443 security levels	Summit framework; NCEES Control Systems exam
Professional Standards and Liability	Engineering ethics, standard of care doctrine, E&O insurance, documentation, owner handoff	NSPE ethics code; Insurance panel
Incident Response and Lifecycle Management	OT incident response, owner handoff, lifecycle maintenance, recertification	CISA; Cheri Caddy frameworks; NIST SP 800-82r3 Ch.5
Capstone / Practicum	Technology Registry, consequence classification, specification, cyber commissioning exercise on real project	HDR, AECOM, Tetra Tech, Michael Baker, UTSI, Johnson Controls, Chinook

Action	Owner — Deadline
Engage GMU representative as WG2 curriculum lead	WG2 Chair — July 2026
Document GMU program as reference model; identify 3 more programs	WG2 — August 2026
Draft ABET petition for cyber safety built-environment program criteria	WG2 — December 2026
Establish practicum partnerships with Summit engineering firms	WG2 + WG1 — Sept 2026
File ABET petition	WG2 — Mid-2027

Q7.3 – What other areas should be addressed? What entities should be involved?

Phase 4

Establish Professional Society Governance

2026–2028

7.4 - The Summit must produce a governance commitment today — not a study of options. One model could be a Multi-Society Consortium led by ISA (technical backbone) with ASCE, IEEE, and ASME as co-signatories, because ISA already owns ISA/IEC 62443 and has ISA99 Committee infrastructure while the other societies provide the PE licensure connection.

The other model is the establishment of a new professional society dedicated to the policies, standards, licensure, certifications, and professional development of cyber safety engineers similar to the Society of Fire Protection Engineers (SFPE) established in 1950. This new society could assume leadership for national implementation of the Cyber-Informed Engineering Strategy as well as advocating for certain controls be mandatory cyber safety requirements for any project.

Action	Owner — Deadline
ISA, ASCE, and IEEE asked for written governance commitment at Summit	Lucian Niemeyer — June 10, 2026
Draft Memorandum of Understanding between consortium members	Legal counsel — Sept, 2026
Draft articles of organization, charter, bi-laws, and leadership/boards for a new non-profit cyber security/safety professional society	
Establish technical committee with representation from: firms, INL, CISA, MITRE, ISA, insurance, academia	WG1 Chair — October 2026
File for ANSI accreditation as standards development body (if new body required)	Consortium lead — Q1 2027
Publish first draft standard for public comment	Consortium — 18 months post-Summit (December 2027)

Q7.4 – What is the preferred path for the establishment of a professional society? What other entities should be involved?

Phase 5

Engage the Insurance Ecosystem

2026–2027

7.5 - The Summit's insurance panelists have the market influence to engage a broader array of brokers and underwriters to determine if the aggregate risk to human safety will translate into support for a cyber safety standard to be economically mandatory within 24 months.

To date, absent a catastrophic event, the insurance industry has not recognized a need to work with cyber security/safety engineers to establish mandatory controls that will mitigate risk to human safety.

The ask is specific: commit to a pilot premium discount program for documented cyber-safe design.

Action	Lead Person — Deadline
Convene WG3 first meeting (Coalition, SAFE Security, ConfigRisk, Observatory) to assess aggregate risk in the built environment	WG3 Chair — July 15, 2026
Produce model cyber safety documentation package for E&O underwriting	WG3 + WG1 — October 2026
Develop professional liability exposure framework: when does failure = negligence?	Need a lead — November 2026
Work with other groups to ensure the controls in 3.3 of this plan are captured in audits and assessments for property and casualty insurance.	
Engage ISO and APCIA for industry-wide underwriting guideline development	WG3 Chair — Q4 2026
Pilot premium discount program for documented cyber-safe design	Coalition (Sezaneh Seymour) or SAFE Security (Steven Schwartz) — June 2027
Publish joint engineering-insurance white paper on OT liability landscape	FDD CCTI + WG3 — December 2026

Q7.5 – What insurance organizations should we engage to start the conversation on cyber safety? What other actions should be taken to collaborate with the insurance industry?

Phase 6

Achieve State Licensure Recognition

2028–2031

Step	Action and Timeline
1 — NCEES CBT Integration (2026–2027)	Per Phase 2. Creates examination infrastructure for licensure.
2 — Model Law Development (2027–2028)	Work with NCEES to draft model law for Cyber Safety Engineer license category, adopted state-by-state.
3 — Pilot State Adoption (2028–2029)	Target: Texas (power/pipelines), Florida (water/ports), Virginia (federal/data centers), California (utilities/transit), New York (finance/infrastructure).
4 — National Rollout (2029–2031)	All 50 states via NCEES model law; coordinate DOE, DHS/CISA, DoD to require licensed Cyber Safety Engineers on federally-funded critical infrastructure.
5 — Federal Mandate (2030+)	Federal procurement requirement for Cyber Safety Engineer of Record on critical infrastructure projects.

Proposed Minimum Licensure Requirements

Requirement	Specification
Education	Accredited engineering degree + cyber safety engineering course sequence (see Phase 3 curriculum) — OR — accredited Cyber Safety Engineering degree (GMU model)
Experience	4 years supervised experience in OT cybersecurity design, specification, or commissioning under a licensed professional
Examination	NCEES FE exam + PE Control Systems exam with cyber safety competency domains (per Phase 2 additions)
Ethics	Professional code of ethics signature with explicit cyber safety obligations
Continuing Education	20 PDH per 2-year cycle; minimum 8 hours annually in current threat landscape updates

Phase 7

Embed in Building Codes and Federal Standards

2028–2033

Standard/Code	Target Change	Lead and Timeline
NCEES PE Exam Sec. 2.D	Add consequence classification, Technology Registry, cyber commissioning, professional duty documentation	WG1 — submit October 2026
ASHRAE Guideline 13-2024	Make Chapter 9 cybersecurity requirements mandatory (not advisory); tie requirements to consequence class	WG1 + ASHRAE TC 1.5 — 2026–2027

ISA/IEC 62443	Coordinate with ISA99 for built-environment-specific guidance; align SL levels to consequence classes	WG1 + ISA99 Committee — ongoing
NIST SP 800-82r3	Request NCCoE built-environment implementation guide referencing Cyber Safety Standard of Care	NIST NCCoE — 2027
International Building Code	Cyber safety annex for Class 3–4 connected buildings, analogous to fire annexes	ICC partnership — 3–5 years
DoD UFGS	Require Cyber Safety Engineer of Record on MILCON projects	ASD Installations — 2027–2029
EPA/State Water Rules	Require cyber safety specification for water/wastewater OT systems	EPA Office of Water — 2028+

Part VIII: The 17 Practical Deliverables

These are the tangible outputs the working groups must produce. The standard has no value without usable artifacts that engineers, owners, insurers, and courts can apply directly.

Priority: These Three Ship First

- Deliverable 2 — Consequence Classification Tool: without it, no one knows if the standard applies
- Deliverable 3 — Technology Registry Template: the foundational document that every other element references
- Deliverable 16 — NCEES Competency Submission: must reach NCEES before October 2026 exam cycle deadline

Deliverable	Working Group	Target Date
1. Model Cyber Safety Standard of Care document	WG1 — Standards	December 2026
2. Consequence Classification Tool (Class 1–4 with decision tree) ★ FIRST	WG1 — Standards	September 2026
3. Technology Registry Template (all required fields) ★ FIRST	WG1 — Standards	September 2026
4. Model Owner Project Requirement (OPR) language	WG1 — Standards	October 2026
5. Model RFP language for cyber safety engineering scope	WG1 — Standards	October 2026
6. Model Cyber Safety Engineer of Record scope of services	WG1 — Standards	October 2026
7. Model Division 01 General Requirements — Cyber Safety clauses	WG1 — Standards	November 2026
8. Model Division 25 Integrated Automation — Cyber Safety clauses	WG1 — Standards	November 2026
9. Cyber Commissioning Checklist (by consequence class)	WG1 — Standards	November 2026
10. Owner Cyber Safety Handoff Checklist	WG1 — Standards	November 2026
11. Model Residual Risk Acceptance Form	WG1 — Standards	November 2026
12. Model Annual Recertification Checklist	WG1 — Standards	December 2026
13. Model Incident Reporting and Post-Incident Review Process	WG1 — Standards	December 2026

14. Insurance Underwriting Questionnaire for OT built-environment	WG3 — Insurance	October 2026
15. Professional Liability Documentation Checklist (E&O claim defensibility)	WG3 — Insurance	November 2026
16. NCEES Competency Submission (Section 2.D additions) ★ FIRST	WG2 — Curriculum	October 2026
17. Continuing Education Syllabus (20 PDH cycle; 8 PDH threat module)	WG2 — Curriculum	December 2026

Part IX: The 90-Day Action Plan

Momentum from a convening dissipates within 30 days without locked-in commitments. Every action below has a named owner and a hard date.

The Rule: If it has no named owner, it will not happen.

Every action in this plan must leave the Summit with a named person responsible — not a working group, not an organization. A person.

Days 1–30 (June 10 – July 10, 2026)

Action	Owner — Hard Date
Publish Summit Declaration with all signatory organizations	Lucian Niemeyer — June 30, 2026
Confirm WG1, WG2, WG3 chairs; distribute charters and 90-day deliverable lists	Lucian Niemeyer — June 30, 2026
Contact NCEES committee staff; request revision cycle timeline and submission requirements	WG1 Chair — July 10, 2026
Confirm WG1 consequence classification model and Technology Registry field structure	WG1 Chair — July 30, 2026
Schedule WG3 first insurance meeting (Coalition, SAFE Security, ConfigRisk, Observatory)	WG3 Chair — July 15, 2026
Brief CISA, ONCD, and DoD; request agency support letters	Lucian Niemeyer + Georgianna Shea — July 30, 2026

Days 31–60 (July 11 – August 9, 2026)

Action	Owner — Hard Date
Produce draft Consequence Classification Tool (Deliverable 2)	WG1 — August 15, 2026

Produce draft Technology Registry Template (Deliverable 3)	WG1 — August 15, 2026
Draft model Division 01 and 25 cyber safety clauses (Deliverables 7, 8)	WG1 — August 31, 2026
Draft Cyber Safety Engineer of Record scope of services (Deliverable 6)	WG1 — August 31, 2026
Engage Prof. Brouse at GMU; identify 3 additional universities for curriculum development	WG2 Chair — August 31, 2026
Draft insurance underwriting questionnaire for OT environments (Deliverable 14)	WG3 — August 31, 2026
Draft MOU for professional society consortium participation	Legal counsel — September 15, 2026

Days 61–90 (August 10 – September 8, 2026)

Action	Owner — Hard Date
Circulate all draft deliverables for stakeholder comment (engineers, owners, insurers, vendors)	All WG chairs — September 30, 2026
Publish Summit White Paper: findings, consensus statements, recommended next steps	FDD CCTI (Georgianna Shea) — September 30, 2026
Launch pilot: one owner + engineering firm + insurer implement Technology Registry and Class 1–4 on one project	WG1 + WG3 — October 2026
Post all model documents to public repository	Building Cyber Security — October 2026
Submit NCEES Section 2.D proposal (Deliverable 16)	Building Cyber Security — October 2026
Schedule December 2026 follow-on convening; distribute progress report template to WG chairs	Lucian Niemeyer — October 2026

Conclusion

> ***"The promise we make to the public must now extend into the digital dimensions of the structures we create.***
>
> *— Opening Address, 2026 Cyber Safety Summit, National Academy of Engineering*

The engineering profession has confronted this moment before and always had a choice: act from within — deliberately, grounded in four thousand years of professional responsibility — or have standards imposed from outside, in haste, after catastrophe. The window to choose the first path is open today.

When the next generation enters a hospital, turns on a water tap, or steps into an automated building — someone must have been accountable for the digital safety of what they are entering. That is the new standard of care. That work begins today.

Appendix A: Working Group Roster

Three working groups form immediately after the Summit. Proposed chairs and members are drawn from confirmed Summit speakers. All chairs must be confirmed by June 30, 2026.

Working Group 1 — Standards Development

Mandate: Produce Deliverables 1–13. Lead the NCEES Section 2.D submission. Drive ASHRAE TC 1.5 and ISA99 engagement.

Name	Organization / Email	Proposed Role
David Brearley	HDR | David.Brearley@hdrinc.com	Proposed WG1 Chair — Global Director OT Cybersecurity
Ben Lampe	Idaho National Laboratory | Benjamin.Lampe@inl.gov	Technical lead — CIE curriculum and NCEES content
Cheri Caddy	Executive Consultant | cheri.caddy@gmail.com	Policy and federal standards integration
Wanda Lenkewich	Chinook Systems | wlenkewich@chinooksystems.com	Cyber commissioning and DoD standards
Shaun Six	UTSI International | scs@utsi.com	OT engineering practice and workforce
John Kliem, PE	Johnson Controls Federal | john.kliem@jcifederal.com	PE perspective; digital transformation integration
Jeff Robertson	Tetra Tech | jeff.robertson@tetratech.com	OT/FRCS cybersecurity engineering
Chuck Weissenborn	Dragos | cweissenborn@dragos.com	ICS/SCADA defense; DoD OT cybersecurity
Alison King	Forescout Technologies | alison.king@forescout.com	Federal/international policy; critical infrastructure
Ari Reubin	KMC Controls | AReubin@kmccontrols.com	Cyber-physical resilience; IoT/BAS integration

Working Group 2 — Curriculum and Licensure

Mandate: Produce Deliverables 16–17. Lead ABET petition. Develop university partnership framework. Drive NCEES model law for Phases 3 and 6.

Name	Organization / Email	Proposed Role

Prof. Peggy Brouse	George Mason University | prouse@gmu.edu	Proposed WG2 Chair — architect of first U.S. Cyber Security Engineering BS
Brian Correia	SANS Institute | bcorreia@sans.org	Continuing education structure; workforce certification
Mark Bristow	MITRE CIPIC | MBRISTOW@mitre.org	Critical infrastructure protection curriculum
Chuck Brooks	Georgetown University | chetz18@icloud.com	Graduate cybersecurity education; risk management curriculum
Tatiana Bolton	Monument Advocacy | tbolton@monumentadvocacy.com	Security by design policy; CSC 2.0 integration
Dr. Georgianna Shea	FDD CCTI | gshea@fdd.org	PCAST contribution; technical content oversight

Working Group 3 — Insurance and Liability

Mandate: Produce Deliverables 14–15. Drive insurance pilot program. Develop professional liability exposure framework. Engage ISO and APCIA.

Name	Organization / Email	Proposed Role
Dan Van Wagenen	Minerva Cyber Technologies | dan.vanwagenen@cybereagle.ai	Proposed WG3 Chair — CTO; DoD cyber background
Sezaneh Seymour	Coalition | sezaneh.seymour@coalitioninc.com	Cyber insurance policy; NSC/regulatory experience
Nick Leiserson	Institute for Security and Technology | nick@securityandtechnology.org	National Cybersecurity Strategy; policy mechanisms
Steven Schwartz	SAFE Security | steven@gofiretower.com	Telemetry-based underwriting; InsurTech innovation
Adam Gladsden	ConfigRisk | contact via LinkedIn or ConfigRisk.com	Construction ecosystem cyber insurance specialist
Gerry Kennedy	Observatory Strategic Management | Gkennedy@observatoryholdings.com	Insurance/resilience/cybersecurity integration
Michael McLaughlin	Buchanan Ingersoll & Rooney | michael.mclaughlin@bipc.com	Professional liability law; negligence framework lead
Jessica Chevraux	AECOM | Jessica.chevreaux@aecom.com	Engineering firm E&O perspective; global practice

Appendix B: Key Standards and References

Obtain these resources before working group sessions begin. Free downloads should be retrieved immediately; purchased standards should be acquired before the first WG meeting.

Standard / Resource	Where to Obtain	Why You Need It
NCEES PE Control Systems CBT Spec (Oct 2022)	ncees.org/exams/pe-exam/control-systems/ — FREE	Read Section 2.D before drafting NCEES submission (WG1, WG2 priority)
ANSI/ISA-62443-2-1-2024	isa.org/standards-and-publications — PURCHASE	Asset owner security program requirements; maps to owner obligations in Part IV
ISA/IEC 62443 Series (full)	isa.org/62443standards — PURCHASE (parts)	Technical backbone; SL 1–4 maps to Consequence Classes 1–4
NIST SP 800-82 Rev. 3 (Sept 2023)	csrc.nist.gov/pubs/sp/800/82/r3/final — FREE	OT consequence-based risk categorization; incident response for safe operation priority
DOE National CIE Strategy (June 2022)	energy.gov/ceser/cyber-informed-engineering — FREE	Engineering logic for building cybersecurity into design; five pillars framework
INL CIE Implementation Guide (Aug 2023)	inl.gov/national-security/cie/ — FREE	Lifecycle application guide; academic curriculum source (WG2 essential)
ASHRAE Guideline 13-2024	ashrae.org/technical-resources/bookstore — PURCHASE	Current BAS specification standard; Chapter 9 is the direct precedent for this standard
NIST CSF 2.0	nist.gov/cyberframework — FREE	Enterprise risk management alignment for owner-facing requirements
2024 PCAST Report on Cyber-Physical Resilience	Search: 2024 PCAST Cyber-Physical Resilience (available via FDD.org) — FREE	Policy authority; Dr. Shea contributed — cite in NCEES and ABET submissions
ABET EAC Engineering Criteria 2025–2026	abet.org/accreditation/accreditation-criteria — FREE	Read before drafting ABET petition (WG2 essential)
GMU BS Cyber Security Engineering program	cybersecurity.gmu.edu — FREE	Reference curriculum model; contact Prof. Brouse (prouse@gmu.edu) for details