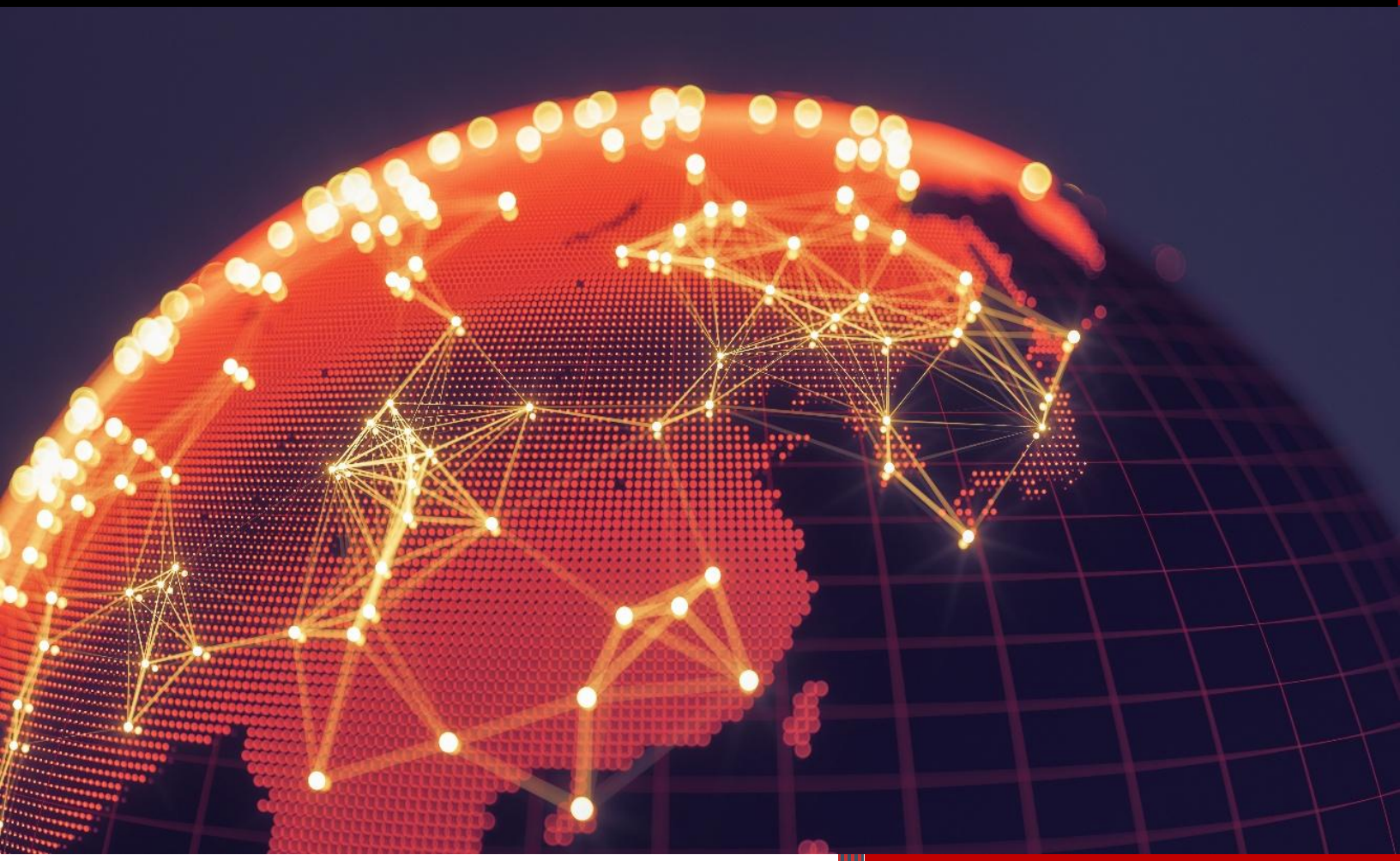
ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

The U.S. Cyber Architecture and Engineering Report Card.



Institute of Security Architecture United
[Project Control-Task Group 61]

Welcome from the Chairman

Cybersecurity has reached the point where configuration work and product marketing are no longer enough. The systems that move money, store health records, operate critical services, and carry public information must be treated as engineered structures, with clear design principles, predictable failure modes, and accountable stewardship. That conviction is why the Institute of Security Architecture United (ISAUnited.org) exists, and why we have chosen to publish a national report card on cyber architecture and engineering.

The U.S. Cyber Architecture and Engineering Report Card 2025 is a first-of-its-kind effort to grade how major U.S. industries design and operate their digital infrastructure. It applies an engineering lens to publicly available evidence, including incidents, disclosures, and sector research. It translates that lens into an accessible A through F grade that the public, policymakers, and executives can understand. The report's research approach is coordinated through the ISAUnited Technical Research Center, which curates source material, applies consistent evaluation logic, and supports technical review to ensure findings are disciplined and defensible. Because the assessment is based on publicly available, independently vetted sources, the grades should be interpreted as sector-level indicators rather than exhaustive measures of every organization. Precision will improve as research partnerships and data science methods mature.

ISAUnited serves as a Security Standards Development Organization focused on cybersecurity architecture and engineering, and this report is one expression of that role. It does not promote products or sell rankings. Instead, it connects observed failures to architectural patterns and, in turn, to the technical standards and design practices that can reduce harm in the years ahead.

Art Chavez
Chairman & Master Fellow
Institute of Security Architecture United (ISAUnited.org)

Divisions of Technical Excellence

ISAUnited is organized into specialized divisions that advance technical rigor, applied education, and disciplined inquiry in cybersecurity architecture and engineering. Each division concentrates expertise in a defined domain and supports research, standards development, and verification activities across our programs. Together, these divisions form the technical engine behind the U.S. Cyber Architecture and Engineering Report Card by providing analysis, scrutiny, and engineering judgment that strengthen the credibility of the findings. They represent the pillars of our Security by Design mission and operate as collaborative centers for innovation and professional advancement across the cybersecurity community.

U.S. Cyber Architecture and Engineering Report Card

Executive Summary

Introduction

America's digital infrastructure is now as critical to daily life as roads, bridges, and power plants. Every payment, medical record update, flight booking, shipment, and public service request depends on an interconnected system of networks, clouds, data platforms, identity fabrics, and monitoring systems. When these systems operate well, they fade into the background. When they fail, the impact is immediate and personal: disrupted services, exposed data, delayed care, financial loss, and erosion of trust. For the public to be safe and for the economy to remain competitive, these systems must be designed and operated as engineered structures, not as loose collections of tools and configurations. Cybersecurity incidents are no longer rare events. They are recurring stress tests of the nation's underlying cyber architecture and engineering practices.

The U.S. Cyber Architecture and Engineering Report Card (U.S. CAE Report Card) provides a national assessment of how well key U.S. industries design, operate, and improve the digital systems that support their critical services. Using a letter-grade A-F format similar to traditional, academic report cards, the U.S. CAE Report Card evaluates the condition and resilience of cyber architectures across sectors and offers practical recommendations to improve those grades over time.

This inaugural edition establishes the scope, grading model, and baseline view of cyber architecture performance in the United States. Future editions will update grades at regular intervals, highlight progress, and highlight areas where systemic weaknesses remain unresolved.

How This Report Is Different

The *ISAUnited Cybersecurity Architecture and Engineering Report Card* is not a third-party vendor report, threat intelligence summary, or analysis of breach statistics. It does not duplicate existing cybersecurity research produced by technology companies, insurers, or commercial consultancies. It is independent and unsponsored, with no commercial influence on scoring or conclusions.

Instead, this report presents original, institute-led findings derived from architecture and engineering evaluations aligned to ISAUnited's Defensible 10 Standards. The grades and observations reflect design quality, engineering rigor, and verification readiness, not incident frequency or attacker behavior.

This approach addresses a long-standing gap in cybersecurity research by evaluating whether organizations are engineered to be defensible by design, rather than measuring outcomes after incidents occur.

Table 01. Comparison Within the Cybersecurity Report Landscape:

Report Type	Primary Focus	Typical Data Sources	What It Explains	What It Does Not Do
Vendor Threat Reports (e.g., breach or threat studies)	Attacker behavior and observed trends	Vendor telemetry, incident response casework, threat feeds	What attacks occurred, how they unfolded, and what techniques were used	Evaluate architecture quality, engineering rigor, or design defensibility.
Breach and Loss Reports	Incident frequency and impact	Public disclosures, regulatory filings, claims data	How often failures occur and the scale of harm	Assess control placement, architectural patterns, or verification readiness.
Workforce and Program Surveys	People, budget, and perceived maturity	Surveys and self-reporting	Organizational constraints and program-level challenges	Validate technical architecture or engineering effectiveness.
ISAUnited Report Card	Architecture and engineering defensibility of digital infrastructure	Practitioner-generated technical evidence and structured evaluations aligned to the Defensible 10 Standards.	Whether systems are engineered to be defensible by design, including failure containment and resilience	Publish threat statistics, rank products, or promote vendors.

Why Compliance Signals Do Not Equal Engineering Defensibility

Over the past decade, many organizations have invested heavily in compliance and assurance programs, including SOC 2, SOC 3, ISO 27001, SOX, and similar vetted assessments. These programs can support governance and reporting, but they are not designed to evaluate whether digital infrastructure is engineered to be defensible under real-world conditions. As a result, strong compliance signals can coexist with architectures that remain fragile under stress, including inbound intrusions and outbound data leaks across commercial enterprises and critical infrastructure.

The U.S. CAE Report Card addresses this gap by evaluating engineering properties that compliance frameworks do not directly measure. These criteria are used to assess the defensibility of digital infrastructure and to explain why grades can differ from what assurance signals might imply:

1. **Failure Containment and Blast Radius Control.**
   Evidence that architectures constrain lateral movement and limit escalation through segmentation, zoning, and controlled pathways across network, cloud, and identity planes.
2. **Trust Boundary and Interconnection Discipline.**
   Evidence that system connections, third-party dependencies, and shared platforms are intentionally designed, governed, and monitored rather than implicitly trusted.
3. **Identity Architecture Correctness.**
   Evidence that identity and access models enforce least privilege, separation of duties, and strong administrative controls across users, workloads, and service identities.
4. **Telemetry, Monitoring, and Verification Readiness.**
   Evidence that logging, detection, and investigative telemetry are sufficient to validate security behavior, support incident reconstruction, and enable verification of corrective action.
5. **Sustainable Remediation Through Design Improvement.**
   Evidence that recurring weaknesses are addressed through architecture changes and engineering corrections, not only through procedural workarounds or compensating controls.

Key Findings

A review of publicly reported incidents, regulatory disclosures, and independent research reveals that America's cyber infrastructure is under significant and persistent stress. While many organizations have invested in security tools and compliance programs, the underlying architecture and engineering of their environments often remain fragile. Several cross-industry themes emerge:

1. **The incident burden on the public remains high and widely distributed.**
   Year after year, breaches and data leaks affect millions of individuals across multiple industries. The problem is not limited to any single sector. Healthcare, financial services, public-sector entities, technology providers, and critical-infrastructure operators all contribute to a steady stream of events that expose sensitive information, disrupt essential services, and necessitate costly recovery efforts.
2. **Design level failures are a recurring cause of serious incidents.**
   Many significant events stem from structural weaknesses rather than isolated configuration errors. Flat or weakly segmented networks, overly permissive identity models, unmanaged third-party connections, poorly governed cloud foundations, and incomplete logging and monitoring are common patterns. These weaknesses allow relatively simple intrusions to escalate into large-scale breaches and outages.
3. **Dependence on third parties and shared platforms is increasing faster than architectural discipline.**
   Organizations across all industries rely heavily on cloud providers, software-as-a-service platforms, managed service providers, and complex supply chains. However, contracts, architectures, and monitoring practices often lag behind this dependency. A compromise in one provider can quickly propagate to many customers, and the design of these interconnections is rarely transparent to the public.
4. **Assurance programs and certifications do not consistently translate into resilient architectures.**
   Many organizations advertise security attestations such as SOC 2 or ISO 27001. These programs have value, but incident patterns show that certified control sets can coexist with fragile architectures. In too many cases, assurance focuses on policy, documentation, and the presence of controls rather than on whether the core system design actually constrains attacker movement and limits blast radius.
5. **Data for architecture level evaluation is still fragmented and incomplete.**
   Public breach portals, incident databases, and regulatory filings provide partial

visibility into how cyber incidents unfold, but there is no consistent national framework for describing architecture level root causes. This limits policymakers', insurers', and the public's ability to understand where systemic structural exposure exists and how it is changing over time.

These findings indicate that the United States needs a sustained, engineering-focused effort to strengthen the design of digital systems, not only the configuration of individual tools.

Grading Scale

The U.S. CAE Report Card uses a simple A through F grading scale to summarize the cyber architecture and engineering posture of each industry sector:

- **A – Exceptional, Engineered to Hold**
  Architectures are generally in excellent condition. Core systems and interconnections are designed with clear security invariants, strong segmentation, disciplined identity patterns, and robust monitoring. Failures still occur but are contained and investigated with high-quality evidence.
- **B – Good, Generally Resilient**
  Architectures are sound overall, with some components or segments showing weaknesses that require attention. Design principles are in place, and most critical systems can tolerate failures without catastrophic impact, although further improvement is needed to address emerging threats.
- **C – Adequate, Vulnerable Under Stress**
  Architectures function and support business operations, but show notable gaps in segmentation, identity design, monitoring, or third-party control. Incidents are more frequent or more severe than expected for the level of investment. Under sustained or coordinated attack, there is a meaningful risk of large-scale impact.
- **D – Weak, High Risk of Serious Failure**
  Architectures are fragmented or outdated, with many critical paths depending on legacy designs, flat networks, or unmanaged connections. Design level weaknesses are a common factor in incidents. The sector is at elevated risk of significant disruption or large-scale data loss.
- **F – Failing, Structurally Unsafe**
  The sector exhibits widespread and severe architectural weaknesses, with frequent serious incidents and limited evidence of effective remediation. Critical services and data are not reliably protected against foreseeable threats.

Grades are not a judgment of individual organizations. They are a sector level signal to the public and to decision makers about structural cyber risk and the urgency of architectural improvement.

About the U.S. CAE Report Card

The U.S. CAE Report Card evaluates a defined set of industries that are central to public life and economic stability, including financial services, healthcare, information technology and cloud providers, energy and utilities, manufacturing and industrial, government and public sector, retail and e-commerce, transportation and logistics, communications, and the third-party and managed service ecosystem.
For each industry, the report card examines:

- The incident footprint that affects people and services in that sector.
- The patterns of failure that point to weaknesses in architecture and design.
- The regulatory and disclosure environment that shapes transparency and accountability.
- The assurance posture, including the use of independent audits and standards.
- The direction of change over recent years, indicating whether resilience is improving or stagnating.

The report is independent and vendor-neutral. It does not sell rankings, sponsorships, or visibility to product vendors or third parties. The focus is on architectures, patterns, and engineering practices, not on tool selection or brand promotion.

Methodology

The U.S. CAE Report Card uses a structured, repeatable methodology that combines quantitative indicators and expert engineering judgement. The approach is inspired by the methodological clarity of established infrastructure report cards and adapted to the realities of cyber systems.

Data sources

The assessment draws solely on publicly available or freely accessible information, including:

- Breach and incident notification portals and public incident databases.
- Regulatory filings and enforcement actions that describe significant cyber events.
- Independent research, sector reports, and longitudinal incident studies.
- Public “trust center” and assurance disclosures from major organizations.
- Technical advisories and analysis from government and independent security bodies.

Evaluation dimensions

To convert raw information into an architecture-focused view, the report scores each industry across five dimensions:

1. Incident Burden – frequency and scale of reported incidents and service disruptions that impact the public.
2. Design Failure Profile – prevalence of incidents driven by structural weaknesses such as flat networks, weak identity fabrics, or unmanaged third-party connections.
3. Regulatory and Disclosure Maturity – transparency of material incidents and presence of systemic findings in regulatory actions.
4. Assurance and Governance Posture – adoption of independent security attestations and breadth of frameworks used to govern cyber risk.
5. Trend and Resilience – direction of change in incidents, design failures, and adoption of modern defensive practices over a multi-year period.

Each dimension is scored on a 0-100 scale, with defined bands that map observed values to subscores. These dimension scores are combined using published weights to produce an overall Cyber Architecture and Engineering (CAE) Score for the sector, which is mapped to an A-F grade.

Before finalizing grades, the results are reviewed by a task group of cybersecurity architects and engineers to ensure that the scores and narratives are consistent with lived practice and do not over- or under-estimate risk.

Recommendations to Raise the Grade

To improve cyber architecture and engineering across U.S. industries, the U.S. CAE Report Card calls for a coordinated agenda built on three pillars: sustained investment in architecture, prioritization of resilient design, and advancement of policies and practices that support the engineering discipline.

1. Sustain Investment in Cyber Architecture and Engineering

Many organizations have invested in tools and compliance programs, but comparatively less in the architecture and engineering capacity required to design environments that can fail safely. Boards, executives, and policymakers should:

- Fund multi-year architecture roadmaps, not only annual tool refresh cycles.
- Support the development and retention of cybersecurity architects and engineers as a recognized discipline.
- Require that major digital transformation and modernization programs include explicit architecture and engineering outcomes, not just feature delivery.

2. Prioritize Resilient Design

Cyber resilience begins with design choices: how networks are segmented, how identity fabrics are built, how data is zoned, and how systems fail under stress. To make environments safer by design, organizations should:

- Treat critical digital systems as engineered structures with clear design requirements, threat models, and failure modes.
- Adopt architecture patterns that contain attacks and limit blast radius, rather than relying solely on detection and response after compromise.
- Incorporate resilience considerations into every major architecture decision, including cloud migrations, new third-party integrations, and adoption of emerging technologies.

3. Advance Policy, Standards, and Evidence-Based Practice

Policy and standards play a vital role in aligning incentives and raising expectations for defensible design. To support better outcomes at scale, leaders should:

- Encourage the use of open, transparent cybersecurity architecture and engineering standards that are independent of specific vendors.
- Improve requirements for root cause disclosure so that material incidents include information about design-level failures where appropriate.

- Promote the use of engineering evidence such as architecture traceability, testing artifacts, and technical computation as part of risk evaluation and insurance underwriting.

Summary

The U.S. Cyber Architecture and Engineering Report Card is intended to shift the national conversation about cybersecurity away from a narrow focus on tools and point solutions and toward how digital infrastructure is designed, connected, and operated as engineered systems.

By grading industry sectors on the defensibility of architecture and engineering and highlighting recurring design patterns behind serious failures, the report card provides the public, policymakers, executives, and practitioners with a clearer picture of where the nation stands and what must change.

A safer digital future for the United States will require sustained investment, disciplined design, and consistent use of engineering standards that treat cyber infrastructure with the same seriousness as physical infrastructure. The U.S. CAE Report Card is one step toward that goal.

End of Document
IO.