ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Protecting People Through Secure Systems for Safer Lives.

ISAUnited's Certified Professional License (CPL)

Institute of Security Architecture United

[Professional Licensing Authority + CPL Governance Working Group]

A Letter to Leaders

Cybersecurity has reached a point where configuration work, product marketing, and compliance narratives are no longer enough. The systems that move money, support patient care, operate critical services, and safeguard public information must be treated as engineered structures. They demand clear design principles, understood failure modes, and accountable stewardship.

That conviction is why the Institute of Security Architecture United exists, and why we developed the ISAUnited Certified Professional License (CPL). CPL was created to make cybersecurity and safety-first an ethos of practice, not a talking point. It sets an enforceable expectation for how cybersecurity architecture and engineering decisions are made, reviewed, verified, and owned.

CPL is built on three elements.

- **Standards** are defined through the ISAUnited Defensible 10 Standards, which establish measurable technical expectations across the core domains of cybersecurity architecture and engineering.
- **Qualifications** validate that a professional can apply those standards with disciplined judgment under responsible charge.
- **Accountability** requires evidence through verification and validation, so security claims are proven, decisions are defensible, and outcomes are reviewable.

This is not a burden a practitioner can carry alone. CPL succeeds when organizations adopt it as a governance commitment. Adoption means leadership assigns responsibility, grants design authority, funds the work, requires verification and validation evidence, and holds risk trade-offs to a disciplined review. When CPL is adopted, accountability is no longer vague. It is defined, visible, and operational.

Secure systems protect people. Safer lives are not accidental outcomes. They are the product of standards, qualified practice, and accountable decisions.

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. These divisions support the ISAUnited Defensible 10 Standards (D10S) and verification and validation practices that provide measurable evidence for CPL adoption. Together, they strengthen CPL through Standards, Qualifications, and Accountability.

Built on Education and Research

CPL is not sustained by credentials alone. It is sustained by disciplined training and defensible technical research. The School of Engineering Cyber Defense develops the practitioner capability required by CPL. The Technical Research Center strengthens CPL credibility by advancing cyber science, validating methods, and supporting evidence-based outcomes.

ISAUnited Technical Research Center
A Division of Applied Cyber Sciences

SCHOOL OF ENGINEERING CYBER DEFENSE

ISAUnited Certified Professional License

Executive Summary

Introduction

The ISAUnited Certified Professional License (CPL) is an evidence-driven licensure program for cybersecurity architecture and engineering practice. It provides organizations with a governance-grade signal of competence for approving security architectures, engineering decisions, and risk trade-offs that affect safety, resilience, privacy, and public trust. CPL is designed for environments where service disruption is unacceptable, including healthcare, education, critical infrastructure, and regulated enterprises. CPL credibility rests on three elements executives can operationalize: Standards, Qualifications, and Accountability.

Why This Matters Now

Cybersecurity failures can disrupt essential services and erode trust at scale. CPL helps leaders distinguish between security activity and security readiness by requiring disciplined practice and verifiable outcomes.

What CPL Is

CPL validates a practitioner's ability to design, build, and govern defensible cybersecurity outcomes under responsible charge. It is evaluation-based and intended for adoption by organizations as part of governance, architecture review, risk acceptance, and assurance processes.

The Three Elements of CPL Credibility

Standards

ISAUnited *technical* Defensible 10 Standards define what "good" looks like for cybersecurity architecture and engineering outcomes. They prove security intent into measurable technical expectations across critical environments, including healthcare, education, and infrastructure.

Qualifications

CPL validates that a professional can apply the standards with discipline, sound judgment, and responsible charge. Qualifications signal verified capability, ethical duty, and ongoing readiness through renewal expectations under Institute governance.

Accountability

Accountability means decisions are owned, defensible, and reviewable, and that security claims are proven through verification and validation. CPL holders and adopting organizations commit to documented trade-offs, measurable evidence, and governance that requires proof of performance beyond compliance alone.

A License for Accountable Practice

Not every cybersecurity role performs architecture and engineering practice. ISAUnited issues the Certified Professional License only to cybersecurity architects and engineers who meet the Institute's eligibility requirements and are prepared to serve as accountable design authority. This posture addresses widespread title inflation and inconsistent role expectations that can leave organizations exposed to avoidable risk. Organizations must not self-appoint practitioners to architect or engineer roles and titles without independent evaluation and clear authority. When systems fail, the impact is not only financial. It can affect safety, privacy, and essential services.

CPL is issued to the right cybersecurity architects and engineers under Institute governance and is not positioned as a pay-to-play, mass-market credential.

What Adoption Looks Like for Organizations

- Assign responsible charge for high-impact security architecture and engineering decisions.
- Adopt a standard of practice for architecture reviews, engineering changes, and risk acceptance.
- Require verification and validation evidence for critical controls, configurations, and operational readiness.
- Integrate CPL expectations into governance gates, procurement, and third-party assurance.

What CPL Means for Practitioners

- Apply ISAUnited standards with disciplined judgment and traceable decision making.
- Translate objectives into measurable requirements and verifiable outcomes.
- Document risk trade-offs, residual acceptance, and corrective actions.
- Support verification and validation that proves controls perform as intended.

Expected Outcomes

- Clearer executive decisions through consistent standards and accountable review.
- Reduced operational disruption through validated security controls and configurations.
- Faster assurance for auditors, partners, and customers because evidence is repeatable and reviewable.
- Increased public trust where continuity and safety are critical.

Recommended Next Steps

Identify systems where a cyber failure would have material consequences for safety, service continuity, privacy, or trust, then assign a responsible charge. Adopting the Defensible 10 Standards for architecture and engineering decisions is crucial and requires verification and validation evidence for critical controls.

Summary

Instituting a *cybersecurity and safety-first* ethos requires more than tools and compliance. It requires qualified architects and engineers operating under responsible charge, backed by governance that demands evidence through verification and validation. CPL enables organizations to adopt that higher standard by aligning their practices with the ISAUnited Defensible 10 Standards and establishing accountable decision-making for systems that matter.

A safer digital future for the United States will require sustained investment, disciplined design, and consistent use of engineering technical standards that treat cyber architecture and infrastructure with the same seriousness as physical infrastructure.

That is why CPL is built on three elements:

Standards - Qualifications - Accountability

End of Document
IO.