WRITTEN TESTIMONY OF LAUREN ZABIEREK and BOB LORD

BEFORE THE HOUSE COMMITTEE ON SMALL BUSINESS
HEARING ON CYBERCRIME AND SMALL BUSINESS SECURITY

December 2, 2025

Chairman, Ranking Member, and Members of the Committee:

Thank you for the opportunity to testify. We, Bob Lord and Lauren Zabierek, respectfully submit this written testimony to the Committee.

While serving at the Cybersecurity and Infrastructure Security Agency (CISA), and together with our colleague Jack Cable, we led the federal government's Secure by Design effort. This work focused on shifting responsibility for cybersecurity upstream to technology manufacturers by promoting software that is safe in its default configuration, rather than relying on small businesses, critical infrastructure operators, and individual users to compensate for inherent design weaknesses.

Our experience at CISA, combined with our backgrounds in national security, software engineering, and public-interest cybersecurity, gave us direct insight into how software design decisions create—or prevent—real-world harm. That perspective informs this testimony and our view that many of the cyber incidents affecting small and under-resourced organizations are rooted in structural properties of the digital ecosystem, not individual negligence.

Today we want to offer our perspective about why cybercrime continues to devastate America's small and medium-sized businesses (SMBs):

> **While conventional wisdom faults the operators with insufficient patching and incorrect configurations, we believe the primary drivers of cybercrime against small businesses are structural, not behavioral. The core vulnerabilities lie in the design of the software ecosystem itself.**

Small businesses are routinely expected to carry responsibilities that exceed their capacity: to secure complex products, maintain patching schedules, manage identity systems, interpret vulnerability advisories, and operate technology in secure configurations that were never designed with them in mind. The result is a persistent asymmetry between attackers—who exploit systemic software weaknesses at scale—and small entities, who absorb the consequence of design decisions they did not make and cannot meaningfully influence.

To illustrate these dynamics, I will walk through three representative examples: a ransomware incident, a data breach, and exploitation of a known, preventable vulnerability.

Each centers on a single, plausible attack vector that demonstrates how insecure-by-default software is the first domino in a chain of harms.

I. Three Real-World Examples of Cybercrime

1.Ransomware: Weak Identity Protections and Unsafe Defaults

A recent national-scale incident illustrates how the absence of fundamental security controls can precipitate cascading societal harm. In this case, an attacker obtained valid credentials, likely exposed in an unrelated breach, and used them to access a remote administrative portal that did not require multi-factor authentication (MFA). The system permitted single-factor login to an environment with expansive operational privileges.

Technically, the compromise was unremarkable. It did not exploit a software vulnerability nor use advanced techniques; the decisive factor was a design choice that treated MFA as optional rather than mandatory for a mission-critical service.

Once authenticated, the attacker deployed ransomware that disrupted healthcare transactions across the country for months. Eligibility checks, claims submissions, and pharmacy benefit queries which are processes relied on by small medical practices, rural clinics, and community pharmacies were rendered unavailable. The downstream effects included delayed care, the diversion of staff to manual workarounds, and significant financial strain on small providers who depend on regular reimbursement cycles.

This incident demonstrates how identity-management design decisions made upstream can have disproportionately harmful consequences for small organizations downstream. The event was rooted not in operational negligence, but in the structural vulnerabilities embedded within widely used software systems.

2. Data Breach: Consequences of Brittle Execution Paths

A second category of incidents involves compromises that begin with a user interacting with a malicious link—a scenario often framed as a training or awareness issue but which, upon closer analysis, reveals deeper architectural weaknesses. In one such incident, yet reminiscent of so many others, an employee at a midsized organization received an email resembling a routine invoice. The message included a hyperlink to what appeared to be a supplier portal. When the employee clicked the link, the browser initiated a sequence of operations that ultimately led to compromise.

We must pause here to stress that despite common narrative that blames the victim, a user clicking on a link or opening a malicious attachment is the *proximate cause*, never the determinative one. Modern browsers routinely process complex and often opaque code originating from untrusted external sources. In this case, the link directed the browser to a site engineered to trigger a known and preventable vulnerability in the browser's JavaScript engine. Modern browsers, despite significant advancements, still expose complex

execution pathways. Inadequate exploit mitigations, memory-unsafe code, and inconsistent sandboxing mechanisms can allow a single user action to escalate into unauthorized access to internal systems.

The attacker used this foothold to exfiltrate sensitive data, including employee and customer information. The incident imposed substantial recovery burdens on the organization and generated collateral harm for several small clients connected to its services.

This example underscores a core principle of human-centered security design: user behavior is predictable, and software systems must be engineered to absorb the consequences of inevitable human actions. When they do not, small organizations bear disproportionate risk.

3.Exploiting Known Vulnerabilities

Another incident that affected hundreds of institutions resulted from the mass exploitation of a well-studied and preventable vulnerability in widely deployed file-transfer software. The flaw, a form of SQL injection, enabled attackers to circumvent authentication and directly extract data from the application's underlying database.

The particular vulnerability could have been prevented in development with secure by design practices, or at least detected before shipping, but was instead discovered by threat actors. Once the vulnerability became public, it was rapidly weaponized. Automated exploitation campaigns compromised organizations across multiple sectors, including state agencies, small businesses, educational institutions, and healthcare entities. Notably, many affected organizations had little visibility into the software's presence within their environments because it operated indirectly through third-party service providers.

The technical mechanism was straightforward: a single defect in an upstream product enabled systematic data exfiltration at scale. The harms were similarly broad—exposure of personal, financial, and health information; notification obligations; loss of public trust; and operational and financial repercussions, particularly acute for small organizations lacking the capacity to absorb such shocks.

This event highlights the systemic interdependence of the modern software ecosystem: a defect in one component can produce widespread downstream harm, irrespective of the security posture of individual small organizations.

II. Cybercrime as Both a Market Failure and a Policy Failure

The through-line across these examples is clear: small entities are harmed because software is shipped with dangerous defaults, recurring classes of coding error, and complex security requirements that small organizations cannot reasonably meet. This is a market failure. But it is also a policy failure.

In other public-safety domains, the United States recognized long ago that market forces alone cannot ensure safety:

- We do not expect consumers to evaluate crash physics before purchasing a car; we require automakers to meet crash-test standards.
- We do not expect passengers to individually assess the integrity of aircraft components; we created the FAA and the NTSB to enforce and investigate aviation safety.
- We do not expect families to independently test their food for contaminants; we empower the FDA to ensure safety before products reach the market.

These systems were built because policymakers acknowledged a fundamental truth: safety is a public good. It cannot depend on individual vigilance or consumer choice.

Software now underpins healthcare, education, transportation, financial services, water utilities, and nearly every domain essential to American life. Yet it remains the only safety-critical domain where we have not established the institutional guardrails such as testing mechanisms, accountability structures, disclosure norms, and incentive frameworks that keep other sectors safe.

Small businesses today occupy a position analogous to drivers before seatbelts, or passengers before modern aviation oversight: they bear risks they cannot see, cannot measure, and cannot mitigate on their own. During our time at CISA, the agency commissioned an economic study from the Research Triangle Institute (RTI) to quantify the magnitude of the negative externalities created by insecure software. Although the final report has not yet been publicly released, a substantial portion of the underlying analysis was presented at the Carnegie Mellon University Secure Software by Design Conference in the summer of 2025. In that presentation, *The Cost of Insecure Software*, the data showed that when aggregating cybersecurity labor costs, spending on cybersecurity products and services, publicly reported cyber incident losses, and cybersecurity insurance, the total economic burden imposed by insecure software across the U.S. economy in 2024 fell between $76.2 billion and $152.8 billion. This range represents uncompensated costs borne by software customers and third parties which are costs largely externalized by software manufacturers. As RTI noted, these are classic negative externalities indicative of a market failure: resources that could otherwise be invested in infrastructure, workforce, and education instead go toward compensating for software that is not safe by design.

RTI's data cannot yet disaggregate how much of this economic burden is borne specifically by SMBs or by state, local, tribal, and territorial (SLTT) governments. However, given that SMBs constitute 99.9% of American businesses and that substantial portions of U.S. critical infrastructure (particularly in water, healthcare, and local government) are operated by SMBs and SLTTs, it is reasonable to infer that these entities shoulder a significant share of the costs. Our intent at the time was to commission a follow-on study to estimate the cost to software manufacturers of building security into products proactively. This would have allowed a comparison between the upstream cost of secure design and the downstream

costs of insecure software, which RTI estimated could reach as high as $152.8 billion annually.

It is important to emphasize that publicly available sources such as the Internet Crime Complaint Center (IC3) substantially understate the true incidence and cost of cybercrime not because of error, but because of structural disincentives to report. In 2024, IC3 recorded 859,532 complaints and $16.6 billion in reported losses. Yet independent research has demonstrated that only a small fraction of actual cyber incidents are reported to law enforcement or centralized complaint systems; many organizations (particularly small businesses and SLTT governments) choose not to report due to fear of reputational damage, legal exposure, regulatory consequence, or because they lack resources to submit complaints. As a result, the IC3 report itself notes that its data reflect "only what the public provides," leaving a substantial "dark figure;" in other words, incidents that go uncounted and unmeasured.

Because the economic cost range estimated by RTI already aggregates both direct and indirect costs, including defensive expenditures, insurance, labor, and incident losses, it likely underestimates the total social cost of software insecurity. The absence of a robust, mandatory reporting infrastructure and the persistent incentives for silence mean that many incidents — especially those impacting small and under-resourced organizations — do not enter any public data stream; in effect, this data deficit is a structural feature of the ecosystem. Until reporting becomes more comprehensive, any quantitative cost estimate must be understood as a conservative lower bound; the true burden is almost certainly higher. Cybercrime should be understood as a significant public-safety problem—one enabled by an absence of the policy infrastructure that protects Americans in every other safety-critical domain.

III. The Federal Context: The Erosion of CISA's Capacity

CISA was created to serve as the connective tissue of the nation's cybersecurity ecosystem—coordinating across sectors, translating federal capabilities to local needs, and acting as the public steward of digital safety. For small businesses and SLTT governments, CISA is often the only federal entity that provides actionable assistance, timely warnings, and a bridge into national cyber defense. Yet over the past year, the parts of CISA most responsible for public-safety functions have been strained by workforce attrition, budget instability, political pressure, and the lack of a confirmed Director to guide CISA's work. This is not simply an operational challenge; it represents a fracture in the federal cyber safety architecture at the very moment small entities face unprecedented exposure.

The erosion of CISA's capacity has weakened several institutional functions that are essential for small and under-resourced organizations:

- Ransomware victim notification, which often determines whether an intrusion becomes catastrophic or recoverable.
- Timely vulnerability advisories, which allow small entities to determine whether they are exposed to known, actively exploited software defects. While CISA's

dedicated personnel continue to issue these advisories, there is a risk that institutional strain may lead to subtle degradations in their frequency, depth, or coordination—effects that would not necessarily be visible from the outside but would nonetheless affect downstream safety.
- Configuration and hardening assistance, which many small organizations rely on because the products they use do not ship securely by default.
- Free scanning and monitoring services, which substitute for tools small organizations cannot afford.
- Sector-specific security support for water systems, rural healthcare providers, school districts, and other critical community institutions.

The concern is that when federal functions are disrupted, the effects can cascade directly onto the weakest nodes in the ecosystem. Small businesses and SLTTs entities without security teams, without redundancy, and without the capacity to absorb operational losses are disproportionately harmed.

The broader implication is clear: no safety-critical domain can function without stable national institutions. Automotive safety requires NHTSA. Aviation safety requires FAA and NTSB. Food safety requires FDA. Digital safety requires CISA, but the parts of CISA that normally fulfill this role are now impaired. This institutional weakening underscores the urgency of rebuilding the federal cyber safety architecture to include reauthorizing CIPAC for structured collaboration, restoring and expanding the Cyber Safety Review Board to learn systematically from incidents, and establishing the independent testing, defect transparency, and liability frameworks necessary for upstream safety. Until these institutional mechanisms are restored and strengthened, small entities will continue to face risks they cannot manage, and the national cyber ecosystem will remain dangerously brittle.

IV. Policy Recommendations

If cybercrime against small businesses reflects both a market failure and a policy failure, then the solution is not more guidance or training—it is the construction of the same structural safety infrastructure that protects Americans in every other safety-critical domain.

1. Modernize the Software Defect Database (CVE Reform)

The CVE system is the closest thing we have to a national software defect database, but it was never designed or resourced to play that role. A modern defect collection framework should incorporate:

- mandatory reporting of software defects that might put paying customers at risk
- consistent defect classification and severity scoring
- richer metadata to enable systemic analysis, and
- clear public reporting, akin to defect dashboards used in automotive safety.

Without reliable visibility into software defects, prevention is impossible.

2. Enable Independent "Crash Testing" Through DMCA Reform and Testing Rights

Safety improves when independent entities can test products without fear of legal retaliation. Automotive safety advanced because researchers could crash-test cars and report the results. Software safety lags because independent testing is often constrained by DMCA §1201 and contractual restrictions.

Congress should legally enable and protect public-interest security testing, supported by:

- A DMCA §1201 carve-out for good-faith testing by independent security researchers, safe harbor for coordinated disclosure, and legislation that would invalidate provisions in EULAs that bar third party reverse engineering and other techniques that help discover software vulnerabilities
- The creation of independent software-safety testing institutions, analogous to the Insurance Institute for Highway Safety. Just as crash-testing transformed automotive safety by revealing real-world failure modes, independent testing of software would provide the empirical evidence needed to identify systemic defects, compare products, and drive industry-wide improvements that voluntary measures alone have not produced

3. Reauthorize and Strengthen the Cyber Safety Review Board (CSRB)

The CSRB was conceived as the digital equivalent of the National Transportation Safety Board: an independent, non-punitive body that conducts rigorous analysis of major cyber incidents. Its mandate to learn from failures and convert incident data into systemic recommendations is essential for national resilience. However, its operations have been disrupted, leaving a vacuum in federal incident-review capacity. No safety-critical sector can improve without a mechanism to learn from failures. Restoring and expanding the CSRB is foundational.

Congress should formally reauthorize and strengthen the CSRB, ensuring:

- Independence from political or commercial pressure
- Authority to review significant cyber incidents affecting SMBs and critical infrastructure,
- Transparent publication of findings, and integration of lessons into federal standards, procurement, and vendor accountability.
- Increased funding and dedicated staff to conduct investigations and issue lessons learned

4. Reauthorize CIPAC as the Nation's Cross-Sector Cyber Collaboration Mechanism

Cybersecurity depends on trust, coordination, and structured public-private communication. For years, the Critical Infrastructure Partnership Advisory Council (CIPAC)

served as the connective tissue between federal agencies, industry, and SLTT partners. Its recent stagnation has left critical gaps in information flow and joint problem-solving. Congress should reauthorize CIPAC, reaffirming its role as a cross-sector engagement mechanism and ensuring that SMBs, sector-specific entities, and local governments have structured pathways into federal cyber decision-making.

5. Introduce Targeted, Modern Liability for Unsafe Software

Liability, when carefully scoped, shifts incentives toward prevention. The aim is to shift the burden from customers to manufacturers—not to punish innovation. Congress should explore:

- Liability for egregious, preventable design flaws,
- Safe-harbor protections for vendors who follow recognized secure-by-design practices
- Baseline obligations for vendors serving critical small-business sectors.

5. Build Minimal but Essential Federal Safety Infrastructure

The objective is not heavy-handed regulation. It is the creation of lightweight but powerful institutional structures that enable safety:

- Defect transparency,
- Independent testing,
- Systemic learning,
- And aligned incentives.

This model mirrors aviation, automotive, and food safety—domains in which safety is achieved not through constant individual vigilance but through institutional competence.

V. Conclusion

Cybercrime against small businesses persists not because they are inattentive, but because they operate in an ecosystem where safety is optional, defects are opaque, and responsibility is misplaced. In every other safety-critical domain, the United States built institutions—testing labs, defect registries, incident review boards, and liability frameworks—that turned dangerous markets into safe ones.

Software has never had those institutions. Small businesses are paying the price. By modernizing defect reporting, enabling independent testing, establishing learn-from-incidents capacity, and aligning incentives through liability, Congress can lay the foundation for a safer digital economy—one where small businesses are not left alone to manage risks they did not create and cannot control.

Thank you. We look forward to your questions.