



APRIL 2021

# THE IMPROVING CONTRACTOR CYBERSECURITY ACT

A Proactive Approach to Securing Federal Networks

**Authored By:**

Drew Spaniel, Lead Researcher, ICIT

Parham Eftekhari, Chairman, ICIT and Senior Vice President and Executive  
Director, the Cybersecurity Collaborative

**Contributions By:**

Dr. Barry West, ICIT Fellow and Former Acting CIO, DHS

Itzik Kotler, ICIT Fellow and Co-Founder and CTO, SafeBreach

James Carder, ICIT Fellow and Chief Security Officer and VP, LogRhythm Labs

Joyce Hunter, Executive Director, ICIT

The potential impact of the SolarWinds breach on public and private sector stakeholders has been the subject of major research publications and media coverage since December 2020. However, SolarWinds was just the most recent in a long line of infamous cybersecurity breaches ranging from OPM to Equifax, all of which occurred when an adversary laterally compromised a system through the vendor supply chain. Emerging legislation proposed by Representative Lieu's office aims to require contractors to assume greater proactive responsibility in securing the solutions they deliver to executive agencies.

### ***About the Improving Contractor Cybersecurity Act of 2021***

The *Improving Contractor Cybersecurity Act*, recently introduced to the 117<sup>th</sup> Congress by Representative Ted Lieu [D-CA], amends the United States Code<sup>1</sup> to require vulnerability disclosure policies and programs from information technology contractors. In other words, the bill would prohibit the head of US executive agencies from entering into contracts with information technology contractors that do not maintain vulnerability disclosure policies for their solutions. James Carder, ICIT Fellow and CSO and VP of LogRhythm Labs, underscores the importance of the legislation, stating, "Our third party vendors haven't been held accountable for ensuring the safety and security of their software. More often than not, they get a pass on having a software development life cycle and a vulnerability management program."

Rep. Lieu's proposed legislation would introduce transparency, accountability, and market incentive into the federal information technology acquisition process. Dr. Barry West, an ICIT Fellow, former government CIO, and current consultant to industry and government, explains, "Having a vulnerability disclosure policy and program will help improve our supply chain and cybersecurity landscape across all of our government systems. This will greatly improve the resiliency of government systems against unknown vulnerabilities by requiring testing, reporting, and timely remediation." The Act specifies that a contractor vulnerability disclosure policy should include:

- A description of the system
- A detailing of the testing for each system that is allowed or specifically not authorized
- A statement that prohibits the disclosure of personally identifiable information (PII) to a third party
- A procedure for individuals to submit vulnerability reports and the ability to do so anonymously

---

<sup>1</sup> Specifically, Chapter 47, Title 41, Division C, Subtitle I

- A commitment that the contractor will not pursue civil action for accidental, good-faith violations of the vulnerability disclosure policy or initiate a complaint to law enforcement for any unintentional violations
- A commitment that the contractor will disclose the name of any entity in compliance with the vulnerability disclosure policy and against whom a suit is brought related to the policy
- A process of verifying the receipt of vulnerability reports and the communication of remediation processes

Last, the policy explicitly should not require PII disclosure or limit testing solely to entities approved by the contractor.

Additionally, the bill requires that disclosed vulnerabilities are evaluated for potential impact and prioritized for action. Vendors are required to collaborate with the researchers who contact them to disclose vulnerabilities and transparently discuss remediation steps and timelines with agencies. Any disclosed vulnerabilities that the contractor is not responsible for patching must be submitted to the Cybersecurity and Infrastructure Security Agency (CISA). CISA will coordinate a vulnerability remediation process with the responsible entity and submit vulnerabilities to the MITRE Common Vulnerabilities and Exposures database and the National Institute of Standards and Technology National Vulnerability Database, as necessary.

## ICIT Fellows' Recommendations for Potential Improvements

When examined by the ICIT Fellows, the *Improving Contractor Cybersecurity Act* only has one shortcoming: the need for additional clarity around scope and further refinement of the internal vulnerability reporting processes.

### Definitions and Scope

Section (1)(A)(i) requires a "description of which system are in scope"; however, ICIT Fellow and SafeBreach Co-Founder Itzik Kotler pointed out that the system in scope may differ from the system in use. Since contractors are defining their systems' scope, they may omit real-world interactions that influence their systems' behaviors. Furthermore, the bill does not include provisions governing the conduct of third and fourth-party stakeholders, such as subcontractors.

In addition to defining the system's scope, the language around timelines for remediation and reporting cycles would benefit from increased specificity. Otherwise, some contractors may meet the letter of the bill, but not the spirit, by perpetuating an endless remediation loop. Finally, the Act does not clearly define what qualifies as a vulnerability, impact, incident, or

breach. As a result, differences in definition could lead to asymmetry in disclosure reporting amongst stakeholders.

### **Internal Vulnerability Reporting Processes**

The bill excels at detailing an external vulnerability disclosure process and includes essential privacy protections, such as the option to report anonymously, indemnity clauses for researchers, and accessibility features, like website reporting. However, internal vulnerability disclosure protections are noticeably absent. These "whistleblower" protections are vital to ensuring that contractors cannot obfuscate or downplay critical vulnerabilities. Furthermore, the bill does not include any clauses preventing the contractor from enforcing an NDA to prevent an internal or external researcher from disclosing a vulnerability.

### ***The Improving Contractor Cybersecurity Act Steps Toward Progress***

Change precipitates from the incremental growth in the direction of progress. Each step on the path to progress appears small but is monumental in its potential to reroute the journey's entire trajectory. Rep. Lieu's *Improving Contractor Cybersecurity Act* does not address every liability or vulnerability in supply chain security. Nevertheless, it is a monumental step in the direction of national supply chain security reform because it institutes an onus of responsibility on federal contractors to secure the solutions they serve to executive agencies.