STATEMENT AND BIO OF

SHANE PAULSEN FRY
CHIEF TECHNOLOGY OFFICER
RUNSAFE SECURITY, INC

BEFORE THE
CYBERSECURITY AND INFRASTRUCTURE PROTECTION
SUBCOMMITTEE
OF THE
HOUSE HOMELAND SECURITY COMMITTEE

AT A HEARING ENTITLED
“DESIGN VS. DEFAULT: ANALYZING SHIFTS IN
CYBERSECURITY”

PRESENTED
DECEMBER 5TH, 2024

STATEMENT OF SHANE PAULSEN FRY, CTO, RUNSAFE SECURITY, INC

Thank you Chairman Green, Subcommittee Chairman Garbarino, Ranking Member Swalwell, and esteemed members of the Committee. I appreciate the opportunity to address the subcommittee today on CISA's Secure by Design initiative.

My name is Shane Fry and I am the Chief Technology Officer of RunSafe Security, having joined the company in 2018 after spending time in the US government and then commercial organizations performing advanced cyber research, both offensive and defensive in nature. I've spent the majority of my career focused in embedded device security, particularly in devices commonly found in critical infrastructure.

Implementing the practices of Secure by Design has helped RunSafe improve the security and reliability of our software, and thus the security and reliability of our customers' systems, which include critical infrastructure and military weapon systems. While we do have a secure software development process, we felt obligated as a security company to port our software to a memory safe language so we would not be the source of an attack on customer systems and networks. It took us approximately 6 months to port our code to Rust, including time to verify correctness of the port and perform extensive testing. Since signing the Secure by Design pledge, we've integrated SBOM generation into our build processes and have plans to host those SBOMs publicly alongside each of our releases. We strongly believe that companies pledging to do Secure by Design should do so as publicly and transparently as possible, and our pledge has accelerated plans to be more public about the security posture of our software.

Secure by Design as a North Star

Secure by Design is a robust program, whose development with aggressive industry engagement increases the chance it shapes product and development practices for decades to come. Instead of companies playing defense on cyber, focusing on chasing every bug, Secure by Design lays out an affirmative series of practices that can decrease the overall risk of devices. It has helped reinforce important cybersecurity concepts like software supply chain security and memory safety, which we'll come back to shortly. It serves its role well as a North Star for software and device developers and its importance can be seen by the large number of companies that have signed the Secure by Design pledge.

The only challenge with a "North Star" is that you never quite reach it. The mechanics for organizations to achieve true, complete Secure by Design can take years or even decades for existing software and systems, risking the program's relevance if "Bridges to Secure by Design" aren't encouraged. The tight, well-researched

recommendations decompose into thousands of complex technical decisions that take years to implement.

Critical Infrastructure Protection

As it pertains to Critical Infrastructure Protection, the elegant vision of Secure by Design meets the reality of legacy hardware, legacy processors, limited system memory, trillions of lines of code, and complex vendor supply chains. Unfortunately, our adversaries won't stop their campaigns of weaponizing our critical infrastructure to achieve their geopolitical objectives while we get our "cyber house" in order. In a hearing before the Select Committee on the Chinese Community Party in January, FBI Director Wray, then-General Nakasone, Director Easterly, and Dr. Coker laid out with stark clarity that China is pre-placing cyber weapons inside our critical infrastructure, in order to disrupt basic citizen services, such as water, transportation, communications, and energy, attempting to divert the political will of the United States from defending Taiwan when China decides to use military action to coerce Taiwan into CCP's system, perhaps between 2027 and 2030. How important will our commitment to Taiwan be if we can't provide clean water to our populace? Director Wray also indicated that if every cyber asset at the FBI was directed to counter China, ignoring all other threats, China's hacking forces would still outnumber the FBI assets 50:1. Companies we're working with in industry have told us it will take 8-15 years, or more, to fully implement aspects of Secure by Design. With 50 times our defensive assets and 8-15 years to continue placing cyber weapons, our critical infrastructure might not be "our" critical infrastructure by the time we are Secure by Design.

Memory Safety

One of the key, but otherwise-esoteric, issues brought to the forefront of cyber hygiene conversations by Secure by Design is "Memory Safety." In recent years, the National Security Agency, the Office of the National Cyber Director, Congress, and CISA have all increased visibility on the endemic risk caused by Memory Safety issues across the economy. In short, Memory Safety issues are when an attacker is able to misuse legitimate software in memory for unintended purposes, arising primarily from systems written in C and C++. By way of an analogy, a memory safety "attack" would be similar to taking the letters, words, and spaces from Little Red Riding Hood and creating a ransom note using those same letters in a different order. Memory Safety attacks take legitimate software and stitch the pieces of the software together in unauthorized ways to hijack the system. As highlighted by the NSA, ONCD, CISA, Microsoft, and many others, memory safety vulnerabilities account for about 70% of the vulnerabilities in C and C++ software. Additionally, according to research by Dr. Laurie Williams at North Carolina State University, this class of vulnerabilities has a

consistently higher vulnerability rating than every other class of vulnerabilities and takes twice as long to fix.

Secure by Design guides critical infrastructure device manufacturers to rewrite all of their C and C++ software into a memory safe language like Rust. For a litany of reasons, that transition to Rust is mechanically impossible within the next five years, leaving our infrastructure exposed to attack. No combination of money, people, or technology exist to achieve that. According to former Gartner analyst Brad LaPorte, now at High Tide Advisors, the cost of rewriting the software can be approximated at between $40 and $70 trillion, based on a comparison to the Y2K problem. There are not enough developers to write or maintain that much Rust. Additionally, the salaries for existing Rust developers tend to be in the top quartile of developer salaries, causing any rewrites to draw on the most constrained and expensive resources. Even if one device manufacturer chooses to write all of their code in Rust, the supporting dependencies in the operating system might not be present in a memory safe language. Even recent studies undertaken by firms at the leading edge of automating code-rewrites from C to Rust indicate that humans are still needed for 95% of the effort, with tools only able to handle 5% of the effort. Finally, there are extensive challenges utilizing memory safe languages in certain critical infrastructure industries where software needs to meet safety certification requirements, for example DO-178 in aviation and ISO 26262 in automotive.

Proposed Solutions

Despite the challenges we've discussed, the committee has many compelling paths forward and CISA's investment in Secure by Design will be essential at each turn. So please allow me to present some suggestions on how industry and government can work together to meaningfully improve the security of critical infrastructure:

1. CISA should modify Secure by Design to incorporate memory protections into existing devices today by encouraging device manufacturers to implement existing commercial solutions that prevent exploitation of devastating memory safety vulnerabilities even without rewriting a single line of code.
2. The US Government should lead by example: US Government developed software should adopt software memory protections today and all funded acquisitions of devices or software should mandate compliance with Secure by Design.
3. Congress should find ways to encourage critical infrastructure asset owners to update software in a timely manner. Assuming every device manufacturer adopts Secure by Design and has secure releases available tomorrow, a huge hole still exists in critical infrastructure: a software update that is secure by default but is never deployed to fielded assets does not make critical infrastructure any more

secure than it is today. None of CISA's current efforts, Secure by Design, Secure by Default, or Secure by Demand address this problem.

4. CISA should include critical infrastructure manufacturers in its Secure by Design Pledge program. For some unexplainable reason, CISA's pledge explicitly excludes physical products, which ends up excluding most critical infrastructure products. The results are clear: none of the major critical infrastructure manufacturers have signed the pledge.
5. Congress should incentivize development of safety certified tooling for DO-178/DO-330 and ISO26262 certification and ISA 62443

Closing

Secure by Design has already had a tremendous impact on industry, but it has a long way to go before we can collectively declare victory. Thank you for the opportunity to testify to this esteemed subcommittee today. I look forward to answering your questions and I appreciate your focus on this very important program.

SHORT BIO OF SHANE PAULSEN FRY, CTO, RUNSAFE SECURITY, INC

Shane Fry is the CTO at RunSafe Security, Inc. He has over a decade of experience in cybersecurity, on both the offensive and defensive sides of the house. Shane began his career performing vulnerability assessments on a variety of software platforms, including Unix/Linux-based operating systems, Mac OS, Android and iOS devices, internet browsers, and cloud computing platforms. His research has spanned all layers of the hardware and software stack, including physical circuit security, secure boot, software update, memory corruption, and web-application vulnerabilities. Shane has worked for the US Government, a large prime contractor, and numerous cybersecurity startups.