SUBJECT: CISA–2023–0027

A response to the Cybersecurity and Infrastructure Security Agency (CISA) Request for Information regarding Secure by Design, in conjunction with the recently published Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software whitepaper.

The Information Technology-Information Sharing and Analysis Center (IT-ISAC) Critical SaaS Special Interest Group (CSaaS SIG) appreciates the opportunity to comment on the *"Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software"* whitepaper from CISA and Secure by Design software practices. For over 20 years, we and our member companies have engaged with the government to improve cybersecurity, threat intelligence sharing, collaboration, and incident response. The CSaaS SIG was formed in 2022 to drive improved security and increase the level of trust that customers can place in the SaaS industry. The SIG enables companies that are essential to the internet to share cyber threat intelligence and effective security practices. These comments reflect our continued commitment to safeguarding critical infrastructure and consumers across the nation.

In a time when cybersecurity is a priority of government and industry, and given the complex threat environment and resource constraints within industry and government, it is important to have a multifaceted approach to cybersecurity. We agree that software and hardware should be designed with security built-in, rather than added on at a later point. However, Secure by Default also is an important component that should not be dismissed. While some use Secure by Design and Secure by Default synonymously, these approaches are related but not interchangeable.

Secure by Design emphasizes incorporating security measures and tactics in a system's design and development phase. Conversely, Secure by Default pushes that the configuration of systems or applications default to secure settings and can be resilient immediately out of the box, enabling the security controls from the onset. We believe that Secure by Default should be the standard in software development, as it ensures a secure product without the user needing additional knowledge to configure it.

In CISA's recent whitepaper, ***Secure by Design, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software***, the authoring organizations state that they "...strongly encourage every technology manufacturer to build their products based on reducing the burden of cybersecurity on customers, including preventing them from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions. We also urge the software manufacturers to build their products in a way that facilitates automation of configuration, monitoring, and routine updates". Many of these same concepts can be applied to the Secure by Default principle.

In 1975, Jerome Saltzer and Michael Schroeder wrote *The Protection of Information in Computer Systems*, in which they outlined eight principles of design. One of these principles included "Fail-safe defaults," which encourages basing access decisions on permission rather than exclusion. This is exactly how Secure by Default programs are built, and this makes customers and/or users aware when they deviate from the default settings – providing an extra layer of security.

While the RFI asks for input on a variety of topics, we are focusing our input on the need to better ingrain cybersecurity into computer science and related fields as a whole. As technology companies with security as a core function of their businesses, and as employers with need for cybersecurity talent, employing people with security skills and knowledge is essential. We therefore offer in these comments the perspective of those looking to hire the next generation of security professionals. Our goal is to emphasize how integrating cybersecurity into curricula at higher education institutions can drive improved security outcomes.

The academic community is a critical partner in elevating the importance of Secure by Default principles, and increasing these principles' understanding and implementation. Evolving the curriculum could assist in bringing this approach more broadly into the workforce while informing the leadership that is at the frontlines of security.

More specifically, there needs to be a shift of expectations and accreditation for computer science and computer information systems degree programs to embed and include computing security in the syllabi of all related courses and materials. Similar to the DevSecOps culture and model, security must be a fundamental attribute of all topics and not a separate or elective subject. We must drive change from the very start of all computer science professionals in order to innately embed this foundational knowledge.

We recommend and would like to ask the pinnacle universities and academia to be change agents in this critical need in the global community. No one academic institution can drive this change on its own. Doing so requires a coalition and united community to start instituting change. It is important to begin as soon as possible since it will take time for multiple generations of university graduates to be fully onboarded and innately educated in the DevSecOps model as their fundamental knowledge base.

In summary, there is tremendous value for higher education institutions to integrate security knowledge and incorporate the DevSecOps model into computer science curricula. Graduates who possess these skills and knowledge will stand out during the hiring process, as it demonstrates their ability to contribute to the organization's security posture from day one. By incorporating security education into computer science programs, universities would be better equipping graduates for the evolving job market and the increasing demand for cybersecurity professionals.

Our more detailed comments and recommendations regarding this topic are as follows:

1.) Continue a nationwide trend towards broader cybersecurity training
Today, a growing number of universities across the United States offer some form of cybersecurity in their curriculum. Graduate-level certificate programs have become a popular way to offer certification to both enrolled students and outside professionals. Degree programs wholly devoted to cybersecurity exist as well, both at the undergraduate and graduate levels. However, these programs only make up a small percentage of the total number of computer

science and computer information systems degrees available. According to CybersecurityGuide.org, there are only 178 cybersecurity degree programs in the United States. And while not every computer science major will want to dedicate themselves to a career in cybersecurity, the principles of these courses are essential for all professionals working in the field.

Yet despite the known importance of cybersecurity, the idea that it should be ingrained into computer science education is still a relatively novel concept. A 2015 Washington Post article criticized the fact that the top ten computer science programs in the country at the time had no mandatory cybersecurity training; three on the list didn't even offer cybersecurity electives. When looking at the major requirements of top computer science programs today, some institutions do offer security courses as part of the main curriculum – however, these courses are often batched in with other possible options on a recommended list, allowing students to select out.

We believe these changes are a step in the right direction, but there is still much to be done to ensure that students receive a suitable standard of cybersecurity training.

2.) Accredited programs should be trailblazers

When it comes to accreditation for computer science programs, modern standards do highlight the importance of training in cybersecurity. The Accreditation Board for Engineering and Technology's 2024-2025 Computing Accreditation Commission Criteria states under Criterion 5 that the computing topics must include "principles and practices of security and privacy in computing," alongside the broader requirement of "techniques, skills, and tools necessary for computing practice." This specific language regarding security and privacy first appeared in the criteria between 2018 and 2019.

To build upon this, we suggest that all Computer Science programs that are accredited should require ongoing cybersecurity lessons throughout their curriculum. The CAC already outlines the importance of security training in their criteria; ongoing education on this topic is a natural step further to ensure that all facets of cybersecurity are covered and reinforced.

3.) Universities should take a holistic approach to cybersecurity education

Though there is a trend toward prioritizing cybersecurity education more and more at the university level, a single course or module in a curriculum is not enough. Cybersecurity is a complex topic covering an immense array of subsections, many of which cannot be distilled down effectively into a short, one-semester class. Rather than try to compile the information into one dose, we recommend educating this topic as a cross-functional requirement, built into the foundation of multiple core classes and the coursework as a whole. This not only allows students to spend more time engaging with each facet of cybersecurity but also places these topics within the context of other modules in the program – highlighting how fundamental security is to all aspects of computer science and the threat landscape we face today.

4.) More security education means safer organizations and products

The need for trained cybersecurity professionals is only growing with time; there are approximately 4 million unfilled cybersecurity jobs worldwide according to data from ISC2. The same data suggests that 52% of cybersecurity professionals begin their careers in other fields and then switch over at a later time; even for students who may think they'll never need a higher-level education in security, career paths may inevitably change especially due to industry needs.

A better base understanding of cybersecurity will serve professionals in the field regardless of where their careers take them; even beyond the scope of cybersecurity-specific jobs, providing students with an understanding of the importance and principles of this topic informs the entirety of the industry moving forward as graduates become professionals. This is precisely our point when it comes to supporting a Secure by Default mindset from education onward: when every designer, developer, and analyst has had sufficient security training at the university level, it's much easier to channel those principles into a more secure product – from inception to release.

5.) Certifications should be supplementary, not mandatory
Though cybersecurity education can be lacking at the university level, that is not to say that professionals are not filling these education gaps themselves. With a lack of education available in the curriculum of traditional computer science programs, many in the industry turn to third-party certifications from organizations such as CompTIA, ISACA, and GIAC. Certifications like these are highly sought by employers; ISC2 data shows that 66% of employers value cybersecurity certifications over a relevant bachelor's degree when considering the ideal candidate. The fact that the degree itself is seen as less valuable than the certification is a case in point: implementing cybersecurity knowledge into degree programs from the beginning can help to remove an extra step in seeking out additional education, and employers can be reassured that candidates who have earned a degree in a computing field have a standardized understanding of cybersecurity principles. Certifications can be exceptionally useful as add-on education, particularly when wanting to specialize deeply in specific topics – but they shouldn't be seen as mandatory prerequisites.

6.) Enterprise should be involved in driving the university curricula
The educational model for a field of study should reflect the needs of the industries in which its graduates are most likely to work. The best way to understand those needs is to encourage organizations themselves to provide feedback and recommendations to academic institutions, helping to drive decisions based on what's needed and relevant at the present moment. Enterprises should work alongside universities in determining curricula, allowing students to be trained in the topics that will best aid them once they graduate and enter the field. This is a mutually beneficial engagement: institutions receive guidance for keeping their syllabi up to date, students receive a more contemporary education based on the needs of their industry, and employers can expect incoming professionals to be better prepared to tackle present issues.

Change at this level can be difficult to implement, but we are optimistic that both industry and academia will recognize the importance of making these necessary adjustments in support of a more security-minded industry overall. As outlined in the Secure by Design whitepaper, one of the main principles of Secure by Design is to "Lead from the top": organizational structure and leadership should seek to enforce and encourage the adoption of this philosophy and maintain security as a priority across all areas of an organization. However, to lead from the top you must have a strong foundation of understanding in place first, and that starts with education. By instilling these principles from the beginning, we can count on more informed future generations of computer science professionals and allow Secure by Default to become the standard framework across industry – leading to safer products, systems, organizations, and customers.

We thank you for the opportunity to share our thoughts on this topic, and for your consideration.