NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

(NIST)

DIGITAL IDENTITY GUIDELINES

REQUEST FOR COMMENT

SUBMISSION

Submitted by

Organization: (ISC)²

Consent: This submission can be made public and published.

(ISC)² is an international nonprofit membership association focused on creating a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of cybersecurity credentials as part of a holistic, effective approach to security. With more than 350,000 members, associates and candidates globally and over 191,000 in the United States, (ISC)² is comprised of certified cyber, information, software and infrastructure security professionals responsible for securing our governments, economies, critical infrastructure and personal information every day.

(ISC)² is a leading authority on the cybersecurity workforce. Annually, (ISC)² conducts the preeminent global Cybersecurity Workforce Study that provides insights into the opportunities and challenges facing the profession. Our most recent report from October 2022, reveals that the global cybersecurity workforce has grown to an estimated 4.7 million. While growth of the workforce is encouraging, unfilled demand for cybersecurity professionals – the global workforce gap – has reached record levels with an estimated unfilled demand for cybersecurity professionals of 3.4 million. In the United States, the estimated cybersecurity workforce increased 5.5% in 2022, to approximately 1.2 million professionals. Despite the growth, unmet need in the U.S. increased to 410,000 workers, an 8.5% increase over 2021.

It's not surprising that demand for cybersecurity professionals is increasing, given an increase in state, federal and global policy and regulatory activities, and high-profile breaches that have garnered fervent media attention. The good news is that through unified collaboration across strategy, policy and global initiatives, the cyber ecosystem can enhance our resilience, bridge the workforce gap, increase diversity within the profession, and create a more safe and secure cyber world.

(ISC)² appreciates the opportunity to submit our researched-based insights to NIST about Digital Identity Guidelines.

We agree with the guidance provided by NIST for enhancements to risk management, identity proofing, authentication, fraud detection and life cycle management. The updates adequately address the processes and technology components necessary for evolving the cyber profession and threat landscape. The guidance could be strengthened with additional recommendations specific to the 'people' component. This would help provide employers with information on the type of individuals to look to with the proper skillsets necessary to translate process and technology into action.

$(ISC)^2$ encourages additional recommendations for employers and others affected by this new guidance to assist them in identifying the cybersecurity expertise they need to comply. These professionals should be qualified by ANSI / ISO / IEC 17024 accredited certification such as the certifications that meet the requirements for eligibility for both the DoD 8140.01 and DoD 8570.01-M.

When considering all guidelines and frameworks for cybersecurity, it is important to ensure the 'people' aspect is included. Only qualified individuals can provide a bridge between the framework, its technical components and its implementation through process improvements and internal controls.

Every successful cybersecurity strategy relies on three essential pillars:

- The first pillar is an understanding that **PEOPLE** are the most essential ingredient in any successful cyber security strategy. This involves ensuring that people are aware of the risks, appreciate how those risks can impact their day-to-day lives and take proactive steps to prevent those risks from eventuating. This involves ensuring that professionals tasked with protecting the information assets of organisations and governments are competent, skilled and certified in being able to do so, which is a significant element of what $(ISC)^2$ as an organisation seeks to achieve. This also involves ensuring that these people have access to relevant resources, training and skills that help to provide timely information in an industry that changes by the second.
- The second pillar is the understanding that **PROCESS** needs to exist when seeking to implement strong cyber security measures. Many of the items listed within the terms of reference for this Inquiry relate to process. The adoption of industry standards for the management of information security systems is critical. Many of the recommendations in the Submission discuss this pillar. However, it is vital to emphasise the point that without the **PEOPLE** in an organisation possessing the right set of knowledge, skills, experience and mindset, any attempt to create processes that minimise the risk will be flawed from the outset. We know this to be self-evident. Consider, for example, mature industries such as aviation where there is no question that best practice dictates that the people working in the sector are competent, skilled and accredited.
- Finally, the third pillar is **TECHNOLOGY**. We all know that this is a high-tech sector. However, $(ISC)^2$ strongly emphasises that the technology functioning as is intended is

entirely dependent on the fact that **PEOPLE** are duly trained, skilled and accredited to deploy, manage and maintain that technology.

We can't stress the importance of having security professionals with knowledge and expertise represented on cybersecurity teams and for those cybersecurity professionals to demonstrate their expertise through globally recognized and accredited certifications. We also encourage more language to be added to the framework that encourages and highlights the importance of certifications particularly as the demands for specialized skills and roles continue to grow.

(ISC)^2 recommends accredited certifications as a mechanism for vetting cybersecurity professionals. Certifications ensure professionals remain up to date with the most current knowledge and education available for their specific area of expertise. For identifying and mitigating risk, the (ISC)^2 CISSP and SSCP as well as CGRC, are examples of certifications applicable for risk management and systems security. Additionally, those holding an (ISC)^2 certification pledge to adhere to a professional code of ethics that includes a requirement to act honorably, justly, responsibly and legally.

The (ISC)^2 CISSP ensures a body of knowledge across a variety of cyber disciplines including security and risk management, identity and access management and security assessment. This certification validates an information security professional's deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization.

CGRC (formerly known as CAP) is a specialized certification and is specifically designed for information security and information assurance practitioners who work in Governance, Risk and Compliance (GRC) roles and have a need to understand, apply and/or implement a risk management program for IT systems within an organization.

The SSCP is a more specialized certification like the CGRC that demonstrates the cybersecurity professional has the advanced technical skills and knowledge to implement, monitor and administer IT infrastructure using security best practices, policies and procedures.

Ensuring the "people" aspect is covered would be our recommendation and that guidance is provided to employers on how to find the most qualified cyber professionals as they endeavor to comply with the new guidance.