(ISC)²®

Chartered Institute of Information Security

Guide to Inclusive Language in Cybersecurity

At **(ISC)²** and the **Chartered Institute of Information Security (CIISec)**, we know that the people within the global cybersecurity profession at large are at the core of everything we do. A diverse and inclusive workforce boosts innovation in solving complex problems facing our world today. In short, having a diverse workforce and fostering an inclusive culture are essential if we are to learn, grow and thrive.

The current cyber workforce gap stands at 3.4 million, and the global cybersecurity workforce still needs to increase by 65% to effectively defend organizations' critical assets. However, a **2021 online survey** found that a lack of diversity and inclusion as well as toxic work cultures were seen as two of the top barriers to entry into the cyber workforce.

To attract as many people as possible to the profession, we need to change those negative perceptions of cyber. That will include changing some of the language, as well as some of the visual cues (e.g., young white man in a hoody), typically used. To begin changing the work culture and to avoid alienating people, the language we use must be inclusive of as many people as possible rather than just a subset.

Expanding the application pool to a much broader range of potential cybersecurity professionals will increase our chances of recruiting a more diverse pool of candidates. This will help us close the workforce gap. Fostering more inclusive environments that allow everyone to bring their authentic self to work is a critical lever that enables more candidates to enter and remain in the profession.

It is clear that our commitment to diversity, equity and inclusion (DEI), both internally and across our industry, is essential to better serve our work and our world. Ensuring that our cyber profession is as inclusive as possible is key to that commitment and therefore to shrinking the workforce gap.

One area that's often overlooked is language – in particular, language that is non-inclusive, alienating a sub-sector of society and portraying people in an unnecessarily negative light.

To ensure that our profession reflects an inclusive culture and shows respect for everyone, we've created an Alternative Vocabulary Guide that replaces non-inclusive terms with more inclusive words and phrases. The terms provided are mostly focused on language surrounding work in the software and information technology fields.

> "The language we use when we write and talk to one another is critical to effective communication. For many of us, our language is something that we have grown up with or that has become embedded in our vocabulary through repetition and culture. However, for some people that language is steeped in negativity that highlights and entrenches inequality, further compounding a system that often creates barriers based on race and ethnicity, gender, sexual orientation and accessibility. It is incumbent on all of us to ensure that we remove those barriers, creating a society that is fairer and equal to all."
>
> **- David Postings, Chief Executive, UK Finance**

Inclusive terminology is just one way to demonstrate commitment to DEI and cultivate a sense of belonging, but it shows that the cybersecurity industry is evolving and committed to removing barriers. Cybersecurity professionals are continually steeped in continuous learning and agility; we invite you to apply that same mindset to both exploring and integrating these more inclusive terms and phrases into your everyday language.

Please keep in mind that the following terms are suggestions; the use of some of them may not be applicable to your organization.

The Alternative Vocabulary Guide is organized into the following categories:

- **Race and Ethnicity**
- **Gender and Orientation**
- **Accessibility**
- **Military and Criminal Justice**
- **Age**

Alternative Vocabulary Guide

Race and Ethnicity

Several terms related to ethnicities, race, culture and racial history were created within contexts of discrimination or persecution. Non-inclusive language (e.g., using the term 'black' to describe something negative and 'white' to describe something positive) can perpetuate negative stereotypes about certain racial or ethnic groups and evoke feelings of alienation or disengagement among individual members.

The terms highlighted below may imply a level of racial bias or discrimination. Suggestions for alternative vocabulary are included with each entry.

- **Black Market:** 'Black Market' is typically used to infer an illegal, underground, or shadow market that operates outside normal rules and regulations, and where the trade of goods or services may be prohibited by law.
Suggested: Illegal Market / Unsanctioned or Underground Economy

- **Blackout Days / Dates; Black / Gray Days:** 'Blackout Days' or 'Blackout Dates' refer to dates where something is inaccessible or denied, e.g., when operations are shut down for maintenance
Suggested: Blocked Days / Restricted Days

- **Master / Slave:** When used together, 'Master' and 'Slave' typically infer some form of dominance, or hierarchy, such as database or server architecture, or backup regime.
Suggested: Primary / Secondary

- **Native:** 'Native' is typically used to describe software that is designed to run on a particular operating system or code written specifically for a certain processor.
Suggested: Built-in

• **White Hat / Black Hat:** 'White Hat' is typically used to refer to an unauthorized user who accesses a system without harmful intent, whilst 'Black Hat' is typically used to infer an unauthorized user that accesses a system with harmful intent. In this context, white is used to describe something that is "good," whilst "black" is something that is bad.

Suggested: Non-Malicious / Malicious or Ethical / Unethical or Authorized / Non-Authorized

• **White Team:** 'White Team' refers to the group responsible for refereeing an engagement between mock attackers / 'Cyber Offense Team' and the 'Blue Team' / defenders of an enterprise's information systems.

Suggested: Cyber Exercise Cell

• **Whitelist / Blacklist:** 'Whitelist' is often used to describe something that is "good" or "allowed" such as an approved list of programs, software or system files that may be allowed access from a computer or device. 'Blacklist' is used to describe something that is "bad" and should be blocked or "denied."

Suggested: Allow List / Block List

• **Yellow Team:** 'Yellow Team' typically is a cybersecurity term referring to the team that builds software (e.g., programmers, application developers, software engineers and software architects, security testers, etc.).

Suggested: DevSecOps Team

Gender and Orientation

Traditionally, society has adopted the “universal male” in terms such as “mankind,” conveying a biased assumption that the default human being is male. This can result in other groups of people feeling irrelevant, invisible and alienated. Additionally, several phrases convey the idea of two genders and one sexuality, which again can cause members of other groups to feel ignored, alienated or disengaged. Additionally, terms that have a sexual connotation may be perceived as vulgar or offensive.

The terms highlighted below have sexual connotations or may imply a level of gender bias or discrimination.

• **Male to Female Connectors:** ‘Male’ or ‘Female’ typically refer to connectors when one or more protrusions from the ‘Male’ connector fit into correspondingindentations in the ‘Female’ connector.
Suggested ‘Male’ alternatives: Plug / Pin / Prong
Suggested ‘Female’ alternatives: Receptacle / Socket / Slot / Jack

• **Man Hours:** ‘Man Hours’ typically refer to hours of a worker’s time.
Suggested: Work Hours / Hours of Effort / Person-Hours

• **Man-in-the-middle:** ‘Man-in-the-middle’ is typically used to infer a type of cyberattack that aims to intercept network communications between two parties; to observe, steal or re-route communications.
Suggested: Network Interception

• **Mom / Girlfriend Test:** ‘Mom Test’ and ‘Girlfriend Test’ refer to the practice of putting a product in front of people who are unfamiliar with it to see how they would use the product.
Suggested: Test With Novice Users / User Test

• **Penetration Testing:** ‘Penetration testing’ typically refers to an authorized security test that simulates a cyberattack in order to see how far an attacker can infiltrate into a network or system without being detected. The test also identifies weaknesses in controls.
Suggested: Ethical Hacking / Security Assessment / Test

• **Virgin:** ‘Virgin,’ when used in a technology context, typically refers to being the first.
Suggested: First Run / First Launch

Accessibility

Non-inclusive language associated with disabilities can contribute to the marginalization of people with disabilities. Terms associated with physical or non-physical disabilities (e.g., 'dumb or 'dummy' have been used to refer to people who cannot speak or who are neurodiverse) can perpetuate stereotypes of weakness, inferiority or abnormality, leading to feelings of alienation or disengagement among members of the relevant group.

The terms highlighted below may imply a level of disability bias or discrimination.

- **Dumb Terminal:** 'Dumb Terminal' typically refers to a terminal's function being confined to the display and input of data in dependence on the host computer for processing power.
  Suggested: Computer Terminal / Terminal / Thin Client

- **Dummy:** Used in technology, 'Dummy' is typically used to imply a lack of knowledge or understanding, of a subject, requiring technical or difficult terms to be explained at a lower level. 'Dummy' can also be utilized in the context of coding to describe a non-functional part of a program.
  Suggested: Beginner

- **Dummy Value:** 'Dummy Value' is typically used to imply known test or sample values for identifier or scheme.
  Suggested: Placeholder Value / Sample Value

- **Sanity Check:** 'Sanity Check' is typically used to imply a test of software or a formula to identify false or unexpected results, mistakes or whether the results are 'rational.'
  Suggested: Functional Test

Military and Criminal Justice

Terms that connotate physical violence or criminal activity can be off-putting to many people, especially those whose lives have been affected by either. The terms highlighted below may imply physical and/or criminal violence.

• **Kill Chain:** 'Cyber Kill Chain' is typically used to explain the different phases of an active cyberattack and the mitigation required to defend and recover from an attack.
Suggested: Attack Chain

• **Wargames:** A 'Wargame' typically simulates a cyberattack in near real-time conditions so that all parties involved can practice the incident response strategy and plan.
Suggested: Tabletop Exercise / Cybersecurity Exercise / Simulation

Age

Terms associated with aging (e.g., "gray") connote negative stereotypes of decline and undesirability, leading to feelings of alienation or disengagement among members of that group. The terms highlighted below may imply a level of age bias or discrimination.

• **Grandfather / Father / Son:**
'Grandfather-Father-Son' is typically used to infer a level of age or hierarchy in infrastructure or backups, where 'Grandfather' is an older generation of technology or backup, and 'Son' is a newer generation or copy. The terms typically infer that 'Grandfather' takes longer to restore whilst 'Son' is quicker to restore.
Suggested: Legacy / Primary

General Language Guidance

General Guidelines When Writing Code or Documentation

Communicating across countries, cultures and languages is now the norm for many organizations. As a result, we all need to keep in mind that both verbal and non-verbal communication will have different connotations for people in different groups.

For this reason, be thoughtful about the imagery you use and be sensitive in your use of symbolism. Consider that some imagery and descriptors hold negative connotations for others and can therefore be offensive.

Regarding verbal communication, a few guiding principles for showing consideration for colleagues and clients from other cultures as well as those who may speak English as their second or third language are included below. In addition, removing non-inclusive language makes your audience much more likely to receive the message you intended to convey:

1. Avoid using terms that have social history. This refers to terms that can have historical significance or impact regarding race, ethnicity, national origin, gender, age, mental and physical ability, sexual orientation, socioeconomic status, religion and educational background.

2. Avoid using acronyms, idioms and jargon. These can exclude people who don't have specialized knowledge and many of these terms don't translate well from country to country or region. You run the risk of alienating or offending others if the idiom does not translate with the same meaning. Additionally, these terms sometimes have origins in negative stereotypes.

3. Be mindful of perpetuating stereotypes or biases. An example of a stereotype is referring to women when discussing individuals who struggles with technology.

4. Check the definitions of words. Some words (e.g., product names) may have vulgar meanings in other languages or may be insensitive from a religious or cultural perspective.

5. Don't use the word "diverse" to describe a person or people. A single person cannot be diverse. Referring to a person as "diverse" is increasingly used as code for people who belong to groups considered on-dominant which in turn makes them an "other."

6. Be cautious when using humor. Some countries have a more formal style to business communications, and jokes could even be perceived as dismissive.

7. Write inclusive examples. Try to avoid using examples in documentation that is culturally-specific to a particular country and be sure to use diverse names.

8. Create automated checks for accessibility using authoring tools. Accessibility Checker is a free tool available in Word, Excel, Outlook, OneNote and PowerPoint on Windows, Office Online, or Mac and Visio on Windows. It finds most accessibility issues and explains why each might be a potential problem for someone with a disability. It also offers suggestions on how to resolve each issue.

9. If you're unsure, ask! Try to be conscious of your language choices. When you are unsure if a particular phrase will cause discomfort, do not hesitate to ask. Most people are happy to walk you through language that makes them feel comfortable and respected.

Additional resources

- Use of Non-Inclusive Language in Technology and Cybersecurity and Why it Matters: Report by UK Finance, EY and Microsoft
https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/uk-finance-language-tech-and-cyber-technical-paper

- The National Cyber Security Centre
https://www.ncsc.gov.uk

About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, nearly 330,000 strong, includes certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – **The Center for Cyber Safety and Education™**. For more information on (ISC)², visit **www.isc2.org**, follow us on **Twitter** or connect with us on **Facebook** and **LinkedIn**.

About CIISec

The Chartered Institute of Information Security (CIISec) was formed in 2006 to advance the professionalism of information security practitioners and thereby the professionalism of the industry. We have a growing membership that represents over 25,000 individuals and provides a universally accepted focal point for the profession, ensuring standards of professionalism for practitioners, qualifications, operating practices, training, and individuals.

CIISec is the natural home for the cyber professional community at every career stage. CIISec's framework-based approach to best practices and skills, gives the industry a way to validate security skills. Our frameworks have been developed in conjunction with industry, government and academia and are aligned with and recognised by other accreditation bodies. The CIISec Skills Framework is widely accepted as the de-facto standard for measuring the competency of Information and Cyber Security professionals.

CIISec offers the CyberEPQ which is the UK's first and only Extended Project Qualification (EPQ) in Cyber Security. This unique Cyber Security qualification has been developed by a consortium of education and Cyber Security partners to help provide a starting point for anyone considering a career in Cyber Security; to go to university, start an apprenticeship or change career.

For more information please visit **www.ciisec.org/** and **cyberepq.org.uk/**

Thank you to all contributors from: