CTPAT Bulletin

May 2020

Cybersecurity – Passwords and Passphrases

(Criterion 4.8)

Last Updated: May 15, 2020

The Customs Trade Partnership Against Terrorism (CTPAT) program is one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to strengthen international supply chains and improve United States border security.

To enhance communication with its Members, CTPAT routinely highlights matters of interest to our membership, from security matters, to recognizing best practices implemented by Members to address supply chain security concerns and challenges.

This CTPAT bulletin highlights the important role that properly constructed passwords and passphrases play in helping maintain a robust cybersecurity posture. Minimum security criterion 4.8, which addresses password requirements, is mandatory and calls for all Members to do three things in order to protect access to their Information Technology (IT) systems:

1. Individuals with access to IT systems must use individually assigned accounts.
2. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.
3. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.

The Implementation Guidance for criterion 4.8 recommends that user access should be granted by going through a two-factor authentication (2FA) or multi-factor authentication (MFA) process. MFA is the most secure because it requires a user to present two or more pieces of evidence (credentials) to authenticate the person's identity during the log-on process. The use of a strong password or passphrase is one type of authentication.

Passwords and passphrases – Passwords are typically composed of not more than 10 letters, numbers and symbols. This is an example of a strong password: AT%^8gr$.

A passphrase, on the other hand, is longer than a password and contains spaces in between words. A passphrase may or may not be a proper sentence; it may simply be four or five words that are not related in any way. The common theme is that a passphrase forces the user to use at a minimum 12 characters, making it basically impossible for a hacking algorithm to guess the passphrase. This is an example of a strong passphrase: Sitting red chair kitchen observe the woods.

Cybersecurity – Passwords and Passphrases

(Criterion 4.8)

Last Updated: May 15, 2020

CTPAT is now recommending that its members use passphrases instead of passwords. This is based on recommendations from experts in both the private and public sector. Here are four reasons why your company should be using passphrases instead of passwords:

1. Passphrases are easier to remember than passwords.
2. Passwords are relatively easy to guess or crack. Online criminals use state of the art hacking tools that allow them to crack even the most complicated passwords. Passphrases, on the other hand, are much harder to crack because password cracking tools break down at around 10 characters.
3. No need to change properly constructed passphrases – unless the user suspects the passphrase has been compromised or a compromise exists.
4. Major operating systems, including Windows, Linux, and Mac, support the use of passphrases, allowing them to be up to 127 characters long.

For those CTPAT Members who choose to continue to use passwords, the following recommendations should be followed to help make those passwords stronger and keep them secure. As per the current National Institute of Standards and Technology's (NIST) guidance, passwords do not need to be changed regularly if these same recommendations are met:

- Don't use passwords that are based on personal information or that can be easily accessed or guessed. Avoid the use of birthdays, names of pets, or favorite movies and books that can be found by a quick search on social networking sites. Users should be prohibited from using their names or the name of the company to construct a password.

- Passwords cannot contain dictionary words.

- Check new and existing passwords against a continually updated database of blacklisted passwords. Regular passwords that are at around 8 characters are still very easy to crack and more and more are being displayed on the dark web as having been cracked. Essentially, they are on blacklists that are used by hackers and also by IT managers to populate their blacklist checkers.

- When the user attempts to enter a new password, that password should automatically be checked by an IT automated system. These IT department checks must be conducted when passwords are created, and continue to be performed on an ongoing basis, preferably daily. These checks should be against a live database, not a static list. A password that was safe yesterday may not be safe today due to a new breach or leak.

- Have a documented process should a password compromise be detected.

- Use different passwords for different accounts.

- Do not allow a user to choose a password that is the same as any of their last four passwords.

Cybersecurity – Passwords and Passphrases

(Criterion 4.8)

Last Updated: May 15, 2020

- Require account login pages to use encryption including a URL address that begins with "https." The “s” indicates a secure or encrypted site instead of "http," which is not encrypted. Look for the padlock icon in the browser bar, too. If the padlock icon appears on the webpage, but not in the browser bar, it might just be a graphic that a cybercriminal embedded to trick you into feeling secure. On top of this, you should move your mouse over the link to look at the address. If there is **any doubt** as to whether or not the site you plan to access is legitimate, contact the company to confirm the actual login page.

Strong passwords and passphrases are undoubtedly essential to security, but they are of no value if users do not learn how to safeguard them and use them wisely. Users must be properly trained on how to generate strong passwords and keep those passwords safe. They must never share their passwords or passphrases with anyone. Do not write passwords on post-it notes and stick them on monitors or other surfaces that are out in the open. If users are unable to remember their passwords, they may write down hints to help them remember them, but these hints must be stored securely, for example, in a locked drawer. One may also use an encrypted password manager. In addition to keeping passwords/phrases secure, never leave one's computing devices unprotected.

Cybersecurity is a shared responsibility. It only takes a single infected computer to potentially compromise thousands and perhaps millions of others. But at the end of the day, cybersecurity is ultimately about people. The most impressive and sophisticated technology is worthless if it’s not operated and maintained by informed and conscientious users. Training your employees in cybersecurity is therefore paramount.

Resources:

STOP. THINK. CONNECT -https://www.stopthinkconnect.org/, this is the global online safety awareness campaign to help all digital citizens stay safer and more secure online.

As the Nation’s risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the Nation’s essentialresources. CISA maintains the National Cyber Awareness System. Its five products offer a variety of information for users with varied technical expertise. A subscription to any or all of the National Cyber Awareness System products ensures that you have access to timely information about security topics and threats. To learn more or to subscribe, visit https://www.us-cert.gov/ncas.

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229

Publication Number: 3720-0524