Transportation Security Administration

SURFACE CYBERSECURITY

AWARENESS GUIDE

STOP | THINK | CONNECT™

INTRODUCTION

It is no longer sufficient to think about cybersecurity as a purely technical problem. Just like physical security, the current threat environment requires a comprehensive approach to cybersecurity risk across your company's operations, including enterprise information technology (IT) and supervisory control and data acquisition (SCADA) systems. As an employee, you must realize the importance of protecting your company's systems from cyber threats because the security of an organization's assets, employees, passengers, cargo and customers depends on it.

TSA'S MISSION

The Transportation Security Administration (TSA) protects the nation's transportation systems to ensure freedom of movement for people and commerce.

Cyber threats originate from a number of places and can adversely affect your business in a variety of ways. It is critical that you and your coworkers are engaged in appropriate practices to avert potentially damaging cyber attacks.

TSA and our surface Transportation Systems Sector (TSS) industry stakeholders are working together to fight terrorism and cybersecurity threats. As part of the cooperative effort to improve surface TSS cybersecurity, TSA has prepared this guide to help you recognize the indications of possible cyber threat activity.

TSA encourages you to refer to this guide and your company's policy and procedures frequently. It is important you know what to do to protect the data on your organization's computer networks.

In This Guide...

This guide outlines the types of threats most commonly found in cyberspace and explains how you can protect your company's data, computer systems and your personal information. It also provides detailed information on the safe use of the Internet, social networks and mobile technology.

WHAT IS CYBERSECURITY?

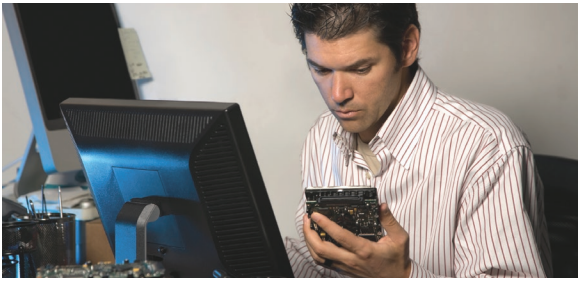
The economic vitality and national security of the U.S. depends on a vast array of interdependent and critical networks, systems, services and resources known as cyberspace. Cyberspace has transformed the way we communicate, travel, power our homes, run our economy and obtain government services.

It is staggering to think about how much of our personal information is stored in computers and therefore at risk of cyber attack. Cyber actors are working day and night to use our dependence on cyberspace against us. These actors present new risks to our economy and national security.

Cyber intrusions and cyber attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations and hurting our economy. Cyber intrusions and attacks fall into two distinct categories, cyber attack (CA) or cyber espionage (CE). The following table defines and gives examples of both a CA and CE.

Cyber Attack (CA)	Cyber Espionage (CE)
→ Any action(s) directed against computers, information systems, networks and/or data stores to disrupt, damage or destroy them → Malware that may delete, alter, corrupt, disrupt or destroy data, files or entire networks	→ Actions taken in cyberspace intended to covertly acquire information and/or to reconnoiter or gain access for attack → Malware that transfers data and hides itself and its activities → Persistent, discreet access to network

Cybersecurity involves protecting the information on which our nation relies by preventing, detecting and responding to attacks.



MYTHS ABOUT CYBER ATTACKS

The Internet is a powerful and useful tool, but in the same way that you shouldn't drive a car without buckling your seat belt or ride a bike without wearing a helmet, you shouldn't venture online without taking some basic precautions. The first step to protecting yourself is to recognize the risks and dispel the myths about cyber attacks, including the following:

Myth: You can't prevent a cyber attack because hackers are geniuses.

Many believe that all cyber actors are expert programmers who can gain access to any computer with a keystroke. In fact, many cyber actors are people who merely exploit known vulnerabilities in your software or operating system or shortcomings in your security practices such as weak passwords. That's why it's important that you quickly apply any update or patch that addresses known vulnerabilities.

Myth: You can always tell when a computer or mobile device has been compromised.

While it's true that some infected computers display unwanted pop-ups or experience performance issues when infected, it is important to remember that cyber actors typically don't want you to know they have access to your files, and they program their viruses accordingly.

Myth: What you do online affects only you.

Because any compromised computer or mobile device can be used to infect others, how you navigate the Internet has the potential to affect others, whether at home, at work or around the world. Practicing good online habits benefits everyone.

MALWARE

Malware is a software that is harmful. Malware can be transmitted through the Internet, email or standard software installation. It is designed to take over infected computer systems and execute unauthorized tasks such as the following:

- Displaying unwanted advertisements
- Accessing unwanted websites
- Tracking online activity
- Stealing passwords and personal information
- Compromising personal accounts
- Crashing computer systems

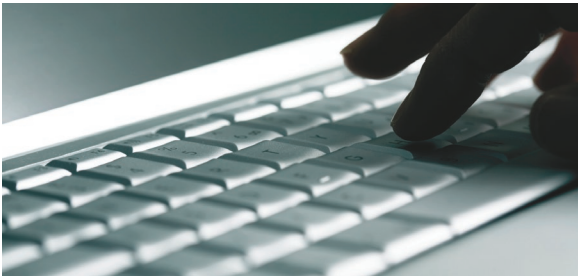
The most common type of malware is called “spyware” or “adware.” Spyware can monitor nearly any activity or information on an infected computer. This includes temporary system data as well as files on the hard drive.

Commonly targeted information includes the following:

- **Email addresses** harvested from an infected computer and used in spam mailing lists
- **Keystroke data** recorded by key loggers before it is sent to the intended application
- **Sensitive information** stored on the system clipboard, including registration codes, data from recently modified documents and personal information that could be used in identity theft
- **Network traffic** monitoring to extract and reconstruct data, including usernames, passwords, email messages and web content

Many viruses act primarily as spyware, while others contain spyware features within them. Common examples include the following:

- **Autonomous spyware** operates as a separate process or injects itself into other processes on a computer system. It can be designed to perform almost any type of function, including email monitoring and giving cyber actors remote access to a computer.
- **Bots** are remote-control agents that give cyber actors access to infected computers as parts of a bot network (botnet). Botnets can scan networks for vulnerabilities, install further malware and harvest personal information, such as passwords, Social Security numbers and banking data.
- **False antispyware tools** are applications available online. They are often advertised as spyware detection or removal tools when, in fact, they themselves are spyware.
- **Hijacking viruses** modify browser settings so that users are directed to unwanted websites.
- **Web bugs** use standard web cookies that store authentication, preferences and other types of user information to track browsing habits and build individual profiles.



PROTECT YOURSELF

Keep a clean machine.
Having the latest security software, web browser and operating system are the best defenses against malware and other online threats. Make sure to keep all your software up to date and to install the latest patches to your operating system, especially those related to network and Internet activity.

Protect all devices that connect to the Internet.
Install trusted antivirus tools and keep them up to date. Computers, tablets, smartphones, gaming consoles and other devices connected to the web all need protection from malware.

Plug and scan.
Universal Serial Bus (USB) keys and other external devices can be infected by malware, so always use your security software to scan them.

Configure your browser and email settings.
Configure your browser to block active content such as ActiveX, Java, scripting, pop-ups and other potentially harmful content. You can also set your email program to send and display email using plain text instead of HTML. This greatly reduces the risks of infection through embedded script, web bugs and other HTML-based techniques. Many email clients now offer the option to disable scripting and block images until the user authorizes their display.

Be mindful of what you download.
Hackers often use social engineering to trick people into installing malware, so exercise caution when downloading anything from public websites or newsgroups. Be especially wary of sites featuring pop-up windows or requests to install browser components and other applications.

Pay attention when installing applications.
If you decide to install an application from the Internet, make sure you read and understand all license and privacy agreements. Information about monitoring functionality and additional software is often included in these documents. During the installation, also make sure to read every instruction, and look out for default options prompting your computer to install additional software. Remember that you are ultimately responsible for what you install on your computer or mobile device.

When in doubt, throw it out.
Links in email, tweets, posts and online advertising are often used to compromise your computer. Regardless of whether you know the source, if it looks suspicious, delete the message or mark it as junk mail.

SPAM & EMAIL SCAMS

Unsolicited commercial email, or spam, is the starting point for many email scams. The wide reach, convenience and anonymity of email allow scammers to work in volume, as they need to fool only a small percentage of the millions of people they contact.

Common email scams include the following:

- **Trojan horse** emails entice you with attachments that might interest you, such as jokes, photographs or patches for a software vulnerability. When opened, however, the attachment may do any of the following:
  - Create a security vulnerability on your computer
  - Give hackers access to your computer and your files
  - Install malware that monitors your online activities
  - Turn your computer into a bot to send spam or spread the virus to other computers
- **False business or investment messages** present the opportunity to make easy money but provide very little detail about the nature of the business. These opportunities usually amount to little more than pyramid schemes encouraging you to recruit more people into the scam or an attempt to get you to browse an unsafe website.
- **Health and diet scams** lure consumers with promises of quick fixes and amazing results for common ailments. The products typically don't work and often serve as an excuse to get you to browse an unsafe website and leave your credit card information.

- **Online con games**, like traditional confidence games, start with an initial bait, such as an email with a personal introduction and a call for an urgent response, and then progress to a series of forged documents and carefully crafted communications asking for money to pay made-up fees or bribes. The purpose of online con games is to trick the victims into transferring funds to the cyber actor or divulging their personal banking information.
- **Phishing** email messages are crafted to look as if they've been sent from a legitimate organization. They often urge you to act quickly because your account has been compromised or your order cannot be fulfilled. The purpose of such email is to fool you into visiting unsafe websites carefully designed to look like the real thing so that you either download malware or reveal sensitive information, such as your account number, your address, your banking username and password, etc.

  If you are unsure whether an email request is legitimate, contact the company directly, using information provided on an account statement or another official document, not the email. Most institutions have policies against asking for personal account information by email, so you should regard any message making such a request with extreme skepticism.

PROTECT YOURSELF

Tips to reduce spam:

Enable filters on your email programs.
Most email clients offer spam filters as well as ways to mark email as spam so that similar messages are no longer delivered to your inbox.

Protect your privacy.
Hide your email address from online profiles and social networking sites, and allow only certain people to view your personal information.

Tips to avoid falling victim to an email scam:

When in doubt, throw it out.
Don't trust any email sent to you by an unknown individual or organization, and never open an attachment to unsolicited email, even if it seems to come from someone you know. Most importantly, never click on a link sent to you by unsolicited email. Instead, delete the email or mark it as junk mail.

Configure your email client for security.
There are a number of ways to configure your email client to minimize the risk of email scams. For example, viewing email as "text only" protects you from scams that use HTML.

Activate your firewall.
A firewall will not prevent scam email from reaching your mailbox, but it can protect your computer if you inadvertently open a virus-bearing attachment. You should also make sure your antivirus software includes an email-scanning feature, and keep it up to date.

Make your passwords long and strong.
Set a different password for every account. To create more secure passwords, combine capital and lowercase letters with numbers and symbols.

Verify the website before sending sensitive information.
Always contact the company directly, using information provided on an account statement or another official document, not the email. Also check the website's URL. Malicious web locations may look identical to the legitimate websites, but their URLs usually have subtle variations in spelling or different domains (such as .com versus .net).

Steps to take if you think you may be the victim of an email scam:

Report the incident.
If applicable, contact your company's network administrators so they can look for any suspicious activity.

Also consider reporting the incident to your local police department and filing a report with the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center.

https://www.ic3.gov/complaint
Phone: **1-800-CALL-FBI (800-225-5324)**

Change your financial accounts.
If you believe your financial accounts may be compromised, contact your financial institution immediately to block any fraudulent transactions. Also close any online account that may have been compromised.

Monitor your financial accounts.
Watch for any unauthorized charges to your financial accounts. Report any suspicious activity immediately. You may have to file a police report as well.

DANGERS ON SOCIAL NETWORKING SITES

Social networking sites such as Facebook and Twitter are a great way to stay connected with others, but you should be wary about how much personal information you post.

Common social networking site threats include the following:

- **Spam and online scams** are similar to email scams. What's more, some sites allow users to hide the URL when posting a link, forcing you to click on it to find out if it's a legitimate address.
- **Fraudulent profiles** are designed to trick you into divulging personal information. Cyber actors create fraudulent profiles to impersonate official organizations or people you know.
- **Data collection** by cyber actors who piece together information from your posts and those of your friends to steal your identity, access your data or stalk you.
- **Hacking accounts** to gain access to your account when you do not guard your username and password carefully. This information can also be stolen from service providers or from your computer or mobile device through malware such as key loggers. Once they have control of your account, cyber actors can do any of the following:
  - Steal any confidential data associated with the account
  - Send out spam and phishing messages to all your contacts
  - View any personal information posted by your contacts
  - Use your name to scam people you know and trick them into divulging personal information

The following are signs that your social networking account has been hacked:

- There are posts on your page you didn't make, such as posts to encourage your friends to click on a link or download an application.
- Users report getting messages or posts that you didn't send.
- Information that was on your social networking account is now gone, lost by way of a data breach, a malware infection or a lost or stolen device.

PROTECT YOURSELF

Tips to keep your information private on social networking sites:

Use the privacy and security settings.
Control who sees what you post and manage the information broadcast about you on social networks. Make sure you read and understand the sites' privacy policies.

Keep your personal information private.
Be cautious about how much personal information you share on social networking sites. Let your friends know if they are posting information about you that you would rather not share. Use the tools available to limit the information to which different groups have access.

Make your passwords long and strong.
Set a different password for each account. Combine capital and lowercase letters with numbers and symbols.

When in doubt, throw It out.
As with email, never trust a message requesting personal information or click on a link from an unsolicited message. If someone is harassing you, block him or her from your friends list and report the situation to the site administrator.

Steps to take if you believe your account has been compromised or hacked:

- **Change the passwords** to all of your related accounts immediately – this is crucial. Remember to set a different password for each account. Combine capital and lowercase letters with numbers and symbols to create a more secure password.

If you cannot access your account because the password has been changed, contact the web service immediately and follow all of their instructions to recover an account.

- **Alert all your contacts** that they may receive spam that will appear to come from your account. Tell them that they should not open messages or click on any links from this account. Warn them of the potential for malware.
- **Scan your computer for malware**. Make sure your security software is up to date and scan your system with an antivirus program.

THREATS TO NETWORKS

Most businesses and households run wireless networks of devices linked to the Internet. This means that every device is connected to a wireless access point controlled by an Internet router. Devices that may connect to a router include the following:

- Computers
- Laptops
- Gaming consoles
- Televisions
- Tablets
- Smartphones
- Printers

To protect these devices and your home from cyber actors, you must ensure that your wireless network is secure.

Common threats to home networks include the following:

- **Piggybacking** occurs when cyber actors in your area connect to your wireless network. This can lead to bandwidth shortages and illegal activity through your Internet connection. That means any crime the hackers commit will be traced back to you.
- **Unauthorized computer access** if your wireless network is not secured. Cyber actors may access files on your computer, install malware or even take control of your computer. They may also monitor your Internet activity to steal passwords and other sensitive information.

PROTECT YOURSELF

Tips to secure your home wireless network:

Make your wireless network invisible.
Identifier broadcasting allows wireless devices to detect your home network as a potential access point. To disable this default option and make your network invisible to others, consult your router's user manual.

Change the router's name and password.
Change your router's default service set identifier (SSID) to a name that cannot be easily guessed. Also, when creating a new password for your router, use a mix of numbers, capital and lowercase letters, and symbols to make sure it is long and strong.

Some routers allow for guests to use the network through a separate password. If you have many visitors to your home, it's a good idea to set up a guest network.

Encrypt your network traffic.
Review your security options and choose the highest level of encryption available. Wi-Fi Protected Access (WPA) and WPA2 are more secure than Wired Equivalent Privacy (WEP).

Activate your firewall.
Most operating systems come with a pre-installed firewall. Make sure to turn it on to block any attempt by cyber actors to access your system.

Use file sharing with caution.
If you don't need to share files on your network, disable file sharing on all your computers. Otherwise, consider creating a single dedicated directory for file sharing and set a strong password for it. Never open your entire hard drive for file sharing.

THREATS TO MOBILE DEVICES

Today's mobile devices are as powerful as any personal computer, so it's important that you take the same security precautions with your smartphone and tablet as you do with your computer.

If you're using wireless technology outside of your home or workplace, you should know about the security threats you may encounter when using a public access point:

- **Evil twin attacks** consist of impersonating an access point to steal data from devices that connect to it. Cyber actors who use this technique can steal a wide range of confidential information, including credit card numbers, addresses, usernames and passwords.
- **Wireless sniffing tools** allow cyber actors to retrieve personal information such as your passwords, bank account numbers and credit card numbers when your device is connected to an unsecure public access point.
- **Shoulder surfing** in public areas allows cyber actors to steal your sensitive information without a computer. If close enough, they can simply glance over your shoulder as you type.

There is also malware specific to mobile devices. Known threats include the following:

- **Smartphone worms** allow cyber actors to hack smartphones from their own mobile devices anywhere in the world. The hackers are then able to do any of the following:
  - Forward financial data stored on your smartphone
  - Coordinate infected smartphones as part of a bot network (botnet)
  - Access your smartphone remotely and change the root password
  - Configure your smartphone to install applications that are not officially distributed or approved by the manufacturer
- **Spy software**, once installed on the target device, allows cyber actors to do any of the following:
  - Listen to phone calls as they happen
  - Secretly read text messages, call logs and email
  - View the device Global Positioning System (GPS) location
  - Forward email to another inbox
  - Remotely control all device functions through text messaging
- **Cross-platform malware**: Any threat affecting your personal computer may have a counterpart for mobile devices. This includes autonomous spyware, bots, hijacking viruses and web bugs.

PROTECT YOURSELF

Tips to protect yourself when using a public wireless access point for your mobile device:

Keep a clean machine.
As with your personal computer, you should install the latest protection on all your mobile devices. Before downloading a new application, make sure you understand its privacy policy and what data it can access.

Protect your personal information.
Give out your cell phone number only to people you know and trust, and never give out anyone else's number without his or her permission. Disable the geotagging feature on your device to keep your usual whereabouts private.

Lock your devices.
Cell phones and other mobile devices often contain a tremendous amount of personal data, and lost or stolen devices can be used to gather information about you and your contacts. Use a strong password to lock your devices.

Consider whether you really need to connect to the Internet.
Disable wireless networking when you are not planning to connect to the Internet.

When possible, connect using a VPN.
Many organizations offer a virtual private network (VPN) that allows employees to connect securely when away from the office. A VPN encrypts your connection and keeps out any unencrypted traffic.

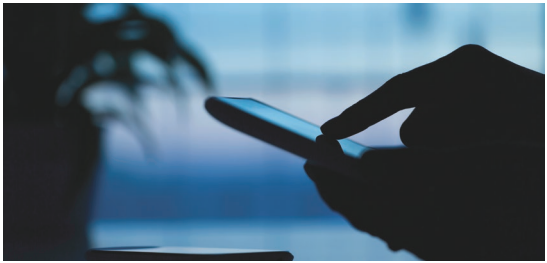
Be careful what you do online.
When choosing your online activities, keep in mind that most public access points offer unsecured, unencrypted network connections. If you can't connect securely using a VPN, consider avoiding the following activities:

- Online banking
- Online shopping
- Sending email
- Typing passwords or credit card numbers

Disable file sharing.
To prevent cyber actors from gaining access to your confidential files, disable file sharing when connecting to a public access point.

Be mindful of your surroundings.
When using a public access point, keep an eye on what's going on around you. Check if others can view your screen.

When in doubt, don't respond.
As with email, never respond to a text, phone call or voice mail requesting your personal information. Using caller ID, you can block all incoming calls from specific names and numbers.



IDENTITY THEFT

Identity theft is when someone steals your personal information and uses it to commit fraud under your name. This serious crime can wreak havoc on your finances, credit history and reputation. There are several types of identity theft, including the following:

- **Tax-related identity theft** is the use of your Social Security number (SSN) to do any of the following:
  - Get a job
  - Apply for government benefits
  - Take your tax refund

  Contact the Internal Revenue Service (IRS) if you receive a notice that you were paid by an employer you don't know or that more than one tax return was filed in your name.

- **Financial identity theft** is the use of your information to do any of the following:
  - Open bank or credit card accounts
  - Apply for loans or utility services
  - Rent a place to live
- **Medical identity theft** is the use of your health insurance information to do any of the following:
  - See a doctor
  - Get prescription drugs
  - File claims with your insurance provider

Medical identity theft can be life-threatening if incorrect information ends up in your personal medical records.

Steps to take if you believe that you are the victim of identity theft:

Change all of your passwords.
Make sure to set a different password for every account. To create more secure passwords, combine capital and lowercase letters with numbers and symbols.

Contact all affected organizations.
This includes any financial institution as well as government organizations. For example, if your SSN and driver's license have been compromised, contact the Social Security Administration (SSA) and your state Department of Motor Vehicles (DMV).

Close or freeze all compromised accounts.
Inform your bank and other financial institutions that someone may be using your identity, and review all recent transactions. Cancel any new account or charge that you did not authorize and obtain new cards with new account numbers.

Contact the authorities.
File a report with your local law enforcement agency. Even if local police don't have jurisdiction over the crime, you will need to provide a copy of the report to your banks, creditors and other businesses. If funds have been stolen, contact one of the three credit bureaus below to place a fraud alert on your file and prevent any further criminal activity.

Equifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

SECURING YOUR DATA

The first step to securing your information is to password-protect your different accounts.

Tips for selecting a password:

- Set a different password for every account.
- Make each password difficult to guess and unique to you.
- Choose at least eight characters, combining capital and lowercase letters with numbers and symbols.
- If you must write down your passwords, store them in a safe place away from the computer.
- Don't share your passwords with others.
- Change your passwords several times a year.

Many account providers now offer additional ways to verify your identity, such as code phrases or user-specific questions. Ask your financial institution and online service providers if they offer multifactor authentication or other supplementary security measures.

BACKING UP YOUR FILES

You should also protect yourself against data loss by making electronic copies of important files. Follow these steps to back up your electronic data:

Keep paper copies of all important documents.
Print out all electronic receipts and other important documents, and file them in a safe place where they would be protected from a natural disaster.

Use your backup software.
Many computers come with software that allows you to make copies of every file and program on your computer. Other software is available for purchase if your system does not have a backup program or if you're seeking other features.

Run your backup program at least once before first connecting to the Internet, and update your backup files at least once per week.

Select a reliable device to store your data.
Store backup files on physical hardware, such as the following:

- CDs, DVDs and USB flash drives: These are best for storing a small quantity of images, music and video files.
- External hard drives: These are best if your computer contains large files or serves as a library for many images, music and video files.

Safely store your backup device.
Keep your backup device somewhere safe, away from the computer. Store it in a place where it would be protected from a natural disaster or any other hazard.

CYBER INCIDENT RESPONSE & RECOVERY

Follow these quick tips if you think you are the victim of a cyber incident:

- If you are at work and have access to an IT department, contact the appropriate staff immediately.
- Verify that the software on all of your systems is up to date. If it isn't, install all appropriate patches to fix known vulnerabilities.
- Disconnect your device from the Internet to prevent cyber actors from accessing your system.
- Update your antivirus program and perform a full scan of your system. If you find an infection, perform a full system restore.
- If you believe sensitive information may have been compromised, notify the appropriate authorities, including your network administrators if applicable.
- File a report with your local police department so that there is an official record of the incident.

DHS CYBER INCIDENT RESPONSE

When cyber incidents occur, DHS provides assistance to potentially affected entities, analyzes the potential impact across critical infrastructure, investigates those responsible in conjunction with law enforcement partners, and coordinates the national response to significant cyber incidents.

DHS works in close coordination with other agencies with complementary cyber missions, as well as private sector and other nonfederal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.

For more information, visit:
www.dhs.gov/cyber-incident-response

National Cybersecurity and Communications Integration Center (NCCIC)

DHS's NCCIC is a 24/7 cyber situational awareness, incident response and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community and law enforcement. The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents and mitigations.

For more information, visit: **www.dhs.gov/national-cybersecurity-and-communications-integration-center**

To report a cyber incident:

Email: **NCCICCUSTOMERSERVICE@hq.dhs.gov**
Phone: **1-888-282-0870**

DHS/TSA RESOURCES

American Public Transportation Association (APTA) Cybersecurity Considerations for Public Transit: This Recommended Practice establishes considerations for public transit chief information officers (CIOs) interested in developing cybersecurity strategies for their organizations. It details practices and standards that address vulnerability assessment and mitigation, system resilience and redundancy, and disaster recovery.

To download, visit **www.apta.com** and search for "Cybersecurity Considerations for Public Transit."

Pipeline Security Guidelines: These guidelines provide security measures for cyber assets and a list of cybersecurity planning and implementation guidance resources for the pipeline industry.

To download, visit **www.tsa.gov/for-industry/surface-transportation** and click on the "Pipeline Security" mode.

Transportation System Sector Cyber Working Group (TSSCWG): This TSA-sponsored public/private joint working group provides a forum for implementing and facilitating national policies, programs, modal outreach, awareness and information sharing.

The group meets monthly and also publishes a weekly newsletter. To be invited, contact: **CyberSecurity@tsa.dhs.gov**

Public Transportation Information Sharing and Analysis Center (PT-ISAC): PT-ISAC is a trusted resource to exchange and share information on physical and cyber threats. The center collects, analyzes and disseminates alerts, incident reports and sector-specific intelligence products, and it helps the government understand sector impacts.

To request access to this free service, contact: **st-isac@surfacetransportationisac.org**

Stop.Think.Connect. Campaign: This national public awareness campaign is aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The campaign includes customized awareness materials for industry, government, law enforcement, small business and others.

For more information, visit: **www.dhs.gov/stopthinkconnect**

Cybersecurity Framework (CSF): The risk-based approach to managing cybersecurity risk allows framework components to reinforce the connection between business drivers and cybersecurity activities. The framework was developed by the National Institute of Standards and Technology (NIST) to complement, not replace, an organization's established risk management process and cybersecurity program.

For more information, visit: **www.nist.gov/cyberframework**

Critical Infrastructure Cyber Community Voluntary Program (C³VP): C³VP supports critical infrastructure owners and operators interested in improving their cyber risk management processes and cyber resilience. It is designed to increase awareness and use of the CSF and to encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management.

For more information, visit: **www.dhs.gov/ccubedvp**

To help address both physical and cyber infrastructure risks, including acts of terror, natural disasters and cyber attacks, President Obama signed Executive Order 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive-21 on Critical Infrastructure Security and Resilience. The Executive Order directed DHS to establish a voluntary program for critical infrastructure cybersecurity to serve as a federal coordination point for cybersecurity resources and to support cyber resilience by promoting use of the CSF.

The C³VP, created in 2014, emphasizes three Cs:

- **Converging** critical infrastructure community resources to support cybersecurity risk management and resilience through use of the CSF
- **Connecting** critical infrastructure stakeholders to the national resilience effort through cyber resilience advocacy, engagement and awareness
- **Coordinating** critical infrastructure cross-sector efforts to maximize national cyber resilience

The C³VP gives state and local governments as well as companies that provide critical services (e.g., cell phones, email, banking and energy) direct access to cybersecurity experts within DHS who have knowledge about the following:

- Specific threats we face
- Ways to counter those threats
- How, over the long term, we can design and build systems that are less vulnerable to cyber threats

For links to C³VP resources, visit:
www.us-cert.gov/ccubedvp

Cyber Risk Management Primer for CEOs: The primer provides key cyber risk management concepts that business leaders should consider. It highlights the five questions business leaders should ask about cyber risks to protect their organizations' systems from cyber threats.

For more information, visit **www.dhs.gov** and search for "Cyber Risk Management Primer for CEOs."

Industrial Control Systems (ICS) Cybersecurity for the C-Level: ICS provides a tool to help facilitate the communication of strong, basic cybersecurity principles to the leadership of ICS/supervisory control and data acquisition (SCADA) organizations. It highlights the six questions business executives should be asking about their organizations' ICS/SCADA.

For more information, visit **https://ics-cert.us-cert.gov** and search for "ICS C-Level."

Cyber Resilience Review (CRR) & Cyber Security Evaluation Tool (CSET): These DHS cyber risk assessments are available as self-assessment downloads. Both serve as a first step for organizations to adopt the CSF, and provide a way for organizations to view/understand the characteristics of their approach to managing cybersecurity risk.

For more information, visit **https://ics-cert.us-cert.gov** and search for "Cyber Resilience Review."

Law Enforcement Cybersecurity Resources: DHS provides a list of recommended support materials for the law enforcement community.

For additional information, visit: **www.dhs.gov/publication/stopthinkconnect-law-enforcement-resources**

DHS Cybersecurity Programs and Resources:

Go to: **www.dhs.gov/topic/cybersecurity**

DHS National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Reporting:

Email: **NCCICCUSTOMERSERVICE@hq.dhs.gov**
Phone: **1-888-282-0870**

CYBERSECURITY QUICK TIPS

Since online technology is constantly evolving, the extent, nature and risks of cyber attacks are impossible to predict. Therefore, it is important that you always take precautions when connecting to the Internet, whether you are at home, at work or in a public place.

Tips to reduce the risk of falling victim to a cyber incident:

- Set strong passwords, change them regularly and don't share them with anyone.
- Keep your operating system, browser and other critical software clean by installing the latest patches and updates.
- Use the available privacy settings and limit the amount of personal information you post online.
- Be mindful of online scams. If it sounds too good to be true, it probably is.

It's also vital to back up your files. This won't shield you from cyber actors, but it will mitigate the effects of any attack.

FEDERAL POCs

Transportation Security Operations Center (TSOC): TSOC provides 24-hour-a-day, 7-day-a-week, 365-day-a-year coordination, communications, intelligence and domain awareness for all DHS transportation-related security activities worldwide. TSOC also:

- Provides continuous domain and operational awareness for TSA Headquarters of special events, incidents and/or crises.
- Furnishes real-time alerting and reporting to field security organizations.
- Fuses actionable intelligence with operational information across all modes of transportation.
- Coordinates with federal, state and local homeland security entities.

To report suspicious activities, call TSOC (also known as the Freedom Center) at **1-866-615-5150** or **1-844-TSA-FRST (844-872-3778)**.

The FBI – Joint Terrorism Task Forces (JTTFs) are small cells of highly trained, locally based investigators, analysts, linguists, SWAT experts and other specialists from dozens of U.S. law enforcement and intelligence agencies.

www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces

FBI Cyber Task Forces: Each FBI field office has highly trained agents who specialize in cyber crime.

www.fbi.gov/investigate/cyber

The **Department of Homeland Security**'s overriding and urgent mission is to lead the unified national effort to secure the country and preserve our freedoms.

www.dhs.gov

Homeland Security Information Network (HSIN): HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified (SBU) information. Federal, state, local, territorial, tribal, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

For more information, contact: **HSIN.Outreach@hq.dhs.gov**

STATE & LOCAL POCs

Agency	Phone Number
Local FBI-JTTF	
Local Fire Department	
Local Police Department	
Emergency Management	
State/Local Fusion Center	
TSA Federal Security Director	

Other Important Contacts	Phone Number

SURFACE CYBERSECURITY

AWARENESS GUIDE

This guide is intended to provide an awareness of specific issues that should be considered when developing and implementing your organization's security plan.

Employees should follow their specific company policies and procedures to prevent, protect and respond to a security incident.

For more information or to request additional complimentary guides, contact TSA at TSA-Surface@tsa.dhs.gov or visit the website at: www.tsa.gov/for-industry/surface-transportation

1-800-361-4653 | www.quickseries.com

01-0804-051-02 | 0804-002
ISBN 978-1-62350-311-6 | Printed in Canada