Cybersecurity Newsletter – Information Sharing Resources

USTRANSCOM is sending you a compilation of sources for a wide range of cybersecurity information. The list contains a mix of programs in which you can enroll as members as well as Websites where you can sign up to receive cybersecurity alerts, advisories, reports, bulletins, and tips.

We know some of you already participate in these programs and have signed up to receive this information, but we want to make sure that everyone is aware of the resources available to you.

USTRANSCOM wants to point out that after you sign up for newsletters and alerts from govdelivery.com, you will receive an email asking that you confirm your request. The email will have the subject "Welcome New User (Confirmation Required)" and will contain a strange looking URL for you to use to confirm your request to get on the distribution list. That URL will take you to the Website so you can confirm your request and add a password to your account. Also, some of the services that you can sign up for on govdelivery.com state that they can only be sent to U.S. Government email addresses. Many of the services do not have that restriction.

Here is the list of cybersecurity information sharing resources:

Cybersecurity and Infrastructure Security Agency (CISA)

CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future. Presidential Policy Directive/PPD-41 designated CISA as the lead federal agency for cyber asset response. Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents. CISA shares knowledge to enable better risk management and protect the Nation's essential resources. Mission priorities include: federal network protection, comprehensive cyber protection, emergency communications, and infrastructure resilience & field operations. This mission requires effective coordination and collaboration among a broad spectrum of local, state, and federal government and private sector organizations.
* Use this link to sign up for email notifications:
https://public.govdelivery.com/accounts/USDHS/subscriber/new

National Cyber Awareness System (NCAS)

NCAS is a CISA service that offers a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.
* Use this link to sign up for email notifications: https://www.us-cert.gov/ncas

CISA Integrated Operations Center (CIOC)

Prior to the establishment of CISA, United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) integrated their independent functions at the National Cybersecurity and Communications Integration Center (NCCIC). As CISA evolved, the NCCIC was reorganized into the CIOC expanding its capabilities while retaining US-CERT & ICS-CERT functions. CIOC acts as a hub for information and expertise and is a global exchange

for cyber and communications information, sharing what they receive back with the cybersecurity community. Information and resources on their website include: incident reporting, vulnerability reporting, sharing indicators and defensive measures, reporting phishing & malware is located at https://www.us-cert.gov/
* Use this link to sign up for email notifications:
https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new

Cyber Information Sharing and Collaboration Program (CISCP)

CISA's Cyber Information Sharing and Collaboration Program (CISCP) enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors. CISCP membership provides access to technical analysts, and to a broad suite of CISA Integrated Operations Center (CIOC) services and products. These resources help reduce the cyberspace attack surface of the United States and its strategic partners and support cybersecurity information exchange.
* Use this link to sign up for email notifications: https://www.cisa.gov/ciscp

Federal Bureau of Investigation (FBI) Cyber Crime

Presidential Policy Directive/PPD-41 designated the FBI as the lead federal agency for cyber threat response which includes criminal investigations and legal attribution. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Our nation's critical infrastructure, including both private and public sector networks, are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators. Just as the FBI transformed itself to better address the terrorist threat after the 9/11 attacks, it is undertaking a similar transformation to address the pervasive and evolving cyber threat. This means enhancing the Cyber Division's investigative capacity to sharpen its focus on intrusions into government and private computer networks.
* Use this link to sign up for email notifications:
https://delivery.fbi.gov/subscribe?utm_source=Email%20Icon%20-%20fbi.gov&utm_medium=Email%20Icon%20-%20fbi.gov&utm_campaign=Email%20Alerts%20Campaign&utm_term=email-alerts&utm_content=Email%20icon%20that%27s%20in%20the%20header%20toolbar%20on%20the%20fbi.gov%20website

InfraGard

InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure. With thousands of vetted members nationally, InfraGard's membership includes business executives, entrepreneurs, military and government officials, computer professionals, academia and state and local law enforcement; each dedicated to contributing industry specific insight and advancing national security.
* Use this link to learn more and sign up for the InfraGard Portal: https://www.infragard.org/

Department of Defense Cyber Crime Center (DC3) DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)

The DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) serves as the single DoD focal point for receiving all cyber incident reporting affecting unclassified networks of DoD contractors from industry and other government agencies. DCISE also serves as the operational focal point for the voluntary Defense Industrial Base Cybersecurity (CS) Program under 32 Code of Federal Regulations part 236 designed to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits, DIB unclassified information systems. DCISE fosters a cyber threat information sharing partnership with DIB participants by performing cyber analysis, offering mitigation and remediation strategies, providing best practices and conducting analyst-to-analyst exchanges with DIB participants.
* Use this link to learn more about the services provided and apply for membership in the program: https://www.dc3.mil/cyber-security

*****You must be a Cleared Defense Contractor to join the DIB CS Program*****

U.S. Maritime Advisories

The U.S. Maritime Advisory System serves as the consolidated U.S. government system for communication with U.S. maritime industry stakeholders regarding potential or observed maritime security threats. This system involves cooperation between U.S. Departments of State, Transportation, Defense, Homeland Security, the Intelligence Community. U.S. Maritime Alerts and Advisories are transmitted by the National Geospatial-Intelligence Agency, emailed to U.S. maritime industry stakeholders, and posted to a web portal to inform mariners of potential maritime security threats. Vessel Masters, Company Security Officers, ship operators, U.S. mariners, U.S. maritime unions and professional associations, and U.S. mariner related non-governmental organizations are the intended recipients of these messages. While U.S. Maritime Alerts and Advisories are transmitted by the National Geospatial-Intelligence Agency and are posted on MARAD-hosted web portal, they should not be referred to as originating from a single agency.

Maritime industry stakeholders who wish to be added to the email distribution list for U.S. Maritime Alerts and Advisories should email their request to MaradSecurity@dot.gov

If you simply want access to the advisories and not sign up for email notifications, follow this link: https://www.maritime.dot.gov/msci-advisories

U.S. Maritime Administration (MARAD)

As the DOT agency responsible for America's waterborne transportation system, the Maritime Administration (MARAD) is busy. At our core, we support the technical aspects of America's maritime transportation infrastructure -- things like ships and shipping, port and vessel operations, national security, environment, and safety. We promote the use of waterborne transportation, and ensure that its infrastructure integrates seamlessly with other methods of transportation. MARAD also maintains a fleet of cargo ships in reserve to provide surge sea-lift during war and national emergencies, and is responsible for disposing of ships in that fleet, as well as other non-combatant Government ships as they become obsolete.
* Use this link to sign up for email notifications:
https://public.govdelivery.com/accounts/USDOTMARAD/subscriber/new
* If you simply want access to the advisories and not sign up for email notifications, follow this link:
https://www.maritime.dot.gov/msci-advisories

US Coast Guard Mandatory Reporting & Marine Safety Information Bulletins (MSIB)

Reporting cyber incidents enables the Coast Guard and other federal agencies to counter cyber threats across the global maritime transportation system. Vessel masters & Maritime Transportation Security Act regulated facilities are required to report suspicious activity, and breaches of security both physical and cyber to the National Response Center (NRC at 800-424-8802), for cyber only events they can alternatively meet reporting requirements by notifying CISA Integrated Operations Center formerly called the NCCIC.
*To access Marine Safety Information Bulletins visit: https://www.dco.uscg.mil/Featured-Content/Mariners/Marine-Safety-Information-Bulletins-MSIB/

National Institute of Standards and Technology (NIST)

The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the nation. NIST's cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.
* Use this link to sign up for email notifications:
https://service.govdelivery.com/accounts/USNIST/subscriber/new

USTRANSCOM Website

The USTRANSCOM Commercial Industry Information Sharing Website is where you can locate historical cyber newsletters, view shared resources, and report an event.

The site can be found at the following link: https://www.ustranscom.mil/cmd/ciis.cfm
Recommendations for information sharing and website content can be sent to the USTRANSCOM Commercial Industry Branch at transcom.scott.tcj3.mbx.j38-comm-component@mail.mil.