U.S. Dept of Homeland Security and Related Internet Resources:

U.S. Department of Homeland Security:

- Learn about issues such as active shooter preparedness, border security, reporting cyber incidents, stopping human trafficking in America to hurricane preparation. Learn and stay informed to prepare and protect yourself, your family and your business from all hazards:
- http://www.dhs.gov/
- http://www.dhs.gov/topics
- http://www.dhs.gov/active-shooter-preparedness

National Infrastructure Protection Plan (NIPP):

- The National Infrastructure Protection Plan (NIPP) provides a unifying framework that integrates a range of efforts designed to enhance the safety of our nation's critical infrastructure. The overarching goal of the NIPP is to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of a terrorist attack or natural disaster, and to strengthen national preparedness, response, and recovery in the event of an emergency.
- http://www.dhs.gov/national-infrastructure-protection-plan

Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience

- The Department of Homeland Security (DHS) leads the Federal government's efforts to secure our **Nation's critical infrastructure by working with owners and operators to prepare for, prevent, mitigate, and** respond to threats. While DHS plays a central role, the Department cannot do this work alone. Public private partnerships are essential. It is through partnerships where the Department continues to see new value and positive impact in mitigating and rapidly responding to crises.
- The EO and PPD-21 reflect the Federal Government's new approach to the critical infrastructure mission, with the concept of critical infrastructure security and resilience (CISR) replacing the notion of critical infrastructure protection (CIP). This change was made because the previous approach — a "left of boom" perspective of protecting against incidents — did not examine the totality of the critical infrastructure picture, which includes prevention, mitigation, response, and recovery. The new approach also fully embraces the All-Hazards mindset, which expands potential causes of disruptive or catastrophic events beyond terrorism. The other major change in approach is that the EO and PPD-21 lay the groundwork for the integration of physical and cyber resilience and security.
- http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical

Food Defense:
FDA works with other government agencies and private sector organizations to help reduce the risk of tampering or other malicious, criminal, or terrorist actions on the food and cosmetic supply.

- http://www.fda.gov/food/fooddefense/
- Get Food Defense and Emergency Coordination updates by E-mail

Homeland Security Information Network (HSIN):
The Homeland Security Information Network (HSIN) is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

HSIN is made up of a growing network of communities, called Communities of Interest (COI). COIs are organized by state organizations, federal organizations, or mission areas such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging and document sharing. HSIN allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate.

To gain access to HSIN-CS (critical sectors), please email your name, employer, work email address, and infrastructure sector (i.e. energy, public health, food, agriculture, transportation, government, etc) you are associated with to:

- CIKRISEAccess@dhs.gov

For general information on HSIN go to:

- http://www.dhs.gov/homeland-security-information-network

NCCIC Weekly Analytic Synopsis Product (WASP) – Cyber Realm
Watch & Warning and Analysis, National Cybersecurity and Communications Integration Center (NCCIC). This weekly publication reports on cyber related attacks, trends, hazards and warnings throughout the United States and the world. It provides analytical information on the event along with mitigating counter measures or advice when necessary.

- NCCIC_WatchandWarning@HQ.DHS.GOV |

Open Source Infrastructure Cyber Read File
The Department of Homeland Security's Industry Engagement and Resilience (IER) branch, part of the Office of Cybersecurity and Communications (CS&C), produces the Open Source Infrastructure Cyber Read File, which is a monthly summary of publicly published information concerning significant cybersecurity and cyber infrastructure issues. Articles at the beginning of each section include context on the open source article to provide additional information and indicate the effect that the article may have on each particular sectors. The CS&C IER Monthly Open Source Infrastructure Cyber Read File is available on the CS&C IER Homeland Security Information. To gain access to HSIN-CS (critical sectors), please email your name, employer, work email address, and infrastructure sector (i.e. energy, public health, food, agriculture, transportation, government, etc) you are associated with to:

- CIKRISEAccess@dhs.gov

DHS Open Source Open Report:
The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. It reports on all infrastructures within the United States and incidents overseas. This is a great summary read resource service for everyday infrastructure owners, operators and staff.

- http://www.dhs.gov/dhs-daily-open-source-infrastructure-report

TRIPwire:
TRIPwire (Technical Resource for Incident Prevention) is a secure, online information-sharing network for law enforcement, bomb squads, and other first responders to learn about current terrorist bombing tactics, techniques, and procedures, including improvised explosive device (IED) design and emplacement.
Sponsored by the Office for Bombing Prevention, TRIPwire serves the bombing prevention community as a consolidated and expert-validated resource of near real-time information on improvised explosives and IEDs, relevant news, and threat alerts.
By combining expert analysis and reports with relevant documents, images, and video gathered directly from terrorist sources, TRIPwire helps homeland security professionals anticipate, identify, and prevent bombing incidents.

- http://www.dhs.gov/tripwire

ICS CERT: The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

- http://ics-cert.us-cert.gov/
- Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009: http://www.us-cert.gov/control_systems/csdocuments.html
- Computer Security Incident Handling Guide, 2008: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

US CERT: United States Computer Emergency Readiness Team

US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. US-CERT's vision is to be a trusted global leader in cybersecurity — collaborative, agile, and responsive in a complex environment.

- http://www.us-cert.gov/

Infrastructure Information Sharing Analysis Center (ISACs):

Information Sharing and Analysis Centers (ISAC) are a concept that was introduced and promulgated pursuant to Presidential Decision Directive 63 (PDD-63), signed May 22, 1998. PDD-63 recognized the potential for the critical infrastructures of the United States to be attacked either through physical or cyber means with the intent to affect the military or economic power of the country. In PDD-63, the federal government asked each critical infrastructure sector to establish sector-specific information sharing organizations to share information, within each sector, about threats and vulnerabilities to that sector. In response, many sectors established "Information Sharing and Analysis Centers" to meet this need. They are trusted entities established by critical infrastructure owners and operators.

Communications ISAC

The National Coordinating Center (NCC) includes as one of its functions the Communications Infrastructure Information Sharing and Analysis Center (Communications ISAC). The Communications ISAC mission is to facilitate voluntary collaboration and information sharing among government and industry in support of Executive Order 12472 and the national critical infrastructure protection goals of Presidential Decision Directive 63 (PDD-63); to gather information on vulnerabilities, threats, intrusions, and anomalies from multiple sources and perform analysis with the goal of averting or mitigating impact upon the telecommunications infrastructure.

- http://www.ncs.gov/ncc/

Electric Sector ISAC

The Electricity Sector Information Sharing and Analysis Center serves the electricity sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions.

- http://www.esisac.com/SitePages/Home.aspx

Emergency Management and Response Information - EMR ISAC

The EMR-ISAC provides the Emergency Services Sector with threat, vulnerability and critical infrastructure protection information through Department of Homeland Security information sharing mechanisms, and provides no-cost technical assistance critical infrastructure protection consultation services to Emergency Services Sector leaders. The Emergency Services Sector (ESS) is representative of the following first-responder disciplines: emergency management, emergency medical services, fire, hazardous material, law enforcement, bomb squads, tactical operations/special weapons assault teams and search and rescue. All first-responders within the ESS are individuals possessing specialized training from one or more of these disciplines.

- http://www.usfa.fema.gov/fireservice/emr-isac/index.shtm

Financial Services ISAC

Launched in 1999, FS-ISAC was established by the financial services sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is now uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information to your organization. This information includes analysis and recommended solutions from leading industry experts.

- https://www.fsisac.com

Information Technology ISAC

Founded in 2000 and achieving operational capability in 2001, the Information Technology . Information Sharing and Analysis Center (IT-ISAC) is a non-profit, limited liability corporation formed by members within the Information Technology sector as a unique and specialized forum for managing risks to their corporations and the IT infrastructure. Members participate in national and homeland security efforts to strengthen the IT infrastructure through cyber information sharing and analysis. As a result, members help their companies improve their incident response through trusted collaboration, analysis, coordination, and drive decision-making by policy makers on cybersecurity, incident response, and information sharing issues.

- https://www.it-isac.org/

Maritime ISAC

The Maritime Security Council (MSC) – established in 1988 – is a non-profit, member-driven organization representing ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters and related maritime industries throughout the world. Our mission is to advance the security of the United States and the international maritime community by representing maritime interests before government bodies; acting as liaison between industry and government;

disseminating timely information; encouraging and assisting in the development of industry-specific technologies; and convening educational and informational conferences for our membership and government partners.

- http://www.maritimesecurity.org/

Multi-State ISAC

The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. The MS-ISAC 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.

MS-ISAC is only a phone call away to assist you with your Incident Response needs by providing you with the following capabilities:

- Malware Analysis
- Computer Forensics
- Network Forensics
- Incident Response
- Onsite Assistance

If you would like to leverage the MS-ISAC for any of the above capabilities, please contact our 7x24 Security Operation Center by calling 1.866.787.4722 or emailing soc@msisac.org. The Incident Response services are available to state, local, tribal and territorial governments. Membership is not required to take advantage of the Incident Response services

- http://msisac.cisecurity.org/

National Health ISAC

NH-ISAC is the nation's Healthcare and Public Health Information Sharing and Analysis Center, responsible for advancing all-hazards (physical and cyber) security national critical infrastructure resilience. Led by the nation's health sector, NH-ISAC is recognized by the US Dept. of Health and Human Services (HHS), the Health Sector-Coordinating Council (SCC), the US Dept. of Homeland Security, the National Institute of Standards & Technology (NIST), Law Enforcement and the National Council of ISACs (NCI Directorate), representing all national critical infrastructures.

- http://www.nhisac.org/

Nuclear ISAC

NEI's Mission: The Nuclear Energy Institute (NEI) is the policy organization of the nuclear energy and technologies industry and participates in both the national and global policy-making process. NEI's objective is to ensure the formation of policies that promote the beneficial uses of nuclear energy and technologies in the United States and around the world.

- http://www.nei.org/

Real Estate ISAC

The Real Estate Information Sharing and Analysis Center (RE-ISAC), a not-for-profit information sharing entity organized by The Real Estate Roundtable in February 2003, is a public-private partnership between the US real estate industry and federal homeland security officials which serves as the primary conduit of terrorism and natural hazard warning and response information between the government and the commercial real estate industry.

- https://portal.reisac.org/SitePages/Index.aspx

Research and Education ISAC

The REN-ISAC mission is to aid and promote cybersecurity operational protection and response within the research and higher education (R&E) communities. The mission is conducted through private information sharing within a community of trusted representatives at member organizations, and as a computer security incident response team (CSIRT) supporting the R&E community at-large. REN-ISAC serves as R&E's trusted partner in commercial, governmental and private information sharing relationships, in the formal U.S. ISAC community, and for served networks.

- http://www.ren-isac.net/

Supply Chain ISAC

The Supply Chain ISAC offers the most comprehensive forum for collaboration on critical security threats, incidents and vulnerabilities to the global supply chain. Its mission is to facilitate communication among supply chain dependent industry stakeholders, foster a partnership between the private and public sectors to share critical information, collect, analyze and disseminate actionable intelligence to help secure the global supply chain, provide an international perspective through private sector subject matter experts and help protect the critical infrastructure of the United States.

- https://secure.sc-investigate.net/SC-ISAC/ISACHome.aspx

Surface Transportation ISAC and Public Transportation ISAC

The ST and PT ISACs are trusted, transportation sector specific, 24/7 Secure Operating capabilities that establish the transportation sector's specific information/ intelligence requirements for incidences, threats and vulnerabilities. Based on its sector focused subject matter analytical expertise, the ST and PT ISACs collect, analyze, and disseminate alerts and incident reports to their membership and help the Government understand impacts for their sector. They provide an electronic trusted ability for the membership to exchange and share information on cyber, physical, and all threats in order to defend critical infrastructure. The ST and PT ISACs provide analytical support to the Government and other ISACs regarding technical sector details and mutual information sharing and assistance during actual or potential sector disruptions.

- The Transit And Rail Intelligence Awareness Daily (TRIAD) Report provides ISAC participants with a quick, easy-to-read synopsis in three fundamental areas – suspicious activities, terrorism and counterterrorism analysis, and general security awareness – with access to more in-depth detail through embedded links to supporting reports. The PT-ISAC also offers additional Cyber Daily Reports, as well as other critical reports.
- http://www.apta.com/Pages/default.aspx
- https://www.surfacetransportationisac.org/

Water ISAC

The Water Information Sharing and Analysis Center (WaterISAC) was authorized by Congress in 2002 and created and managed by the water sector. Its mission is to keep drinking water and wastewater utility managers informed about potential risks to the nation's water infrastructure from contamination, terrorism and cyber threats. The mission has been expanded to help utilities respond to and recover from all hazards. Funded by membership fees and matching federal funds, WaterISAC links members through a secure online portal. The Member base includes water utilities and state and federal agencies dealing with security, law enforcement, intelligence, the environment and public health.

- https://portal.waterisac.org/home