CIAware

Awareness Through Information Sharing

Incidents/Articles of Note:

- IG: DoD Did Not Properly Secure Access to VIP Records
- State of Resilience: Critical Infrastructure and the 9/11 Commission Report
- CISA Must Update Critical Infrastructure Protection Plans
- Critical infrastructure warrants mandatory safeguards and sufficient funding
- ICS Vulnerabilities Increased by 41% In Six Months Amidst High Profile Attacks on Critical Infrastructure
- Forbes: Critical Infrastructure Providers Need To Shape Up And Focus On Cybersecurity

- Tools and Resources -

Video Resource | Carnegie Endowment

Countering Cyber Threats to Critical Infrastructure: What's Next?

From shuttered gas stations and disrupted chemotherapy treatments to the near-poisoning of a small town's water supply, in the past year the public felt the impact of cyber threats to critical infrastructure like never before. Fortunately, leaders in government and the private sector responded swiftly and effectively to secure the systems that underpin our daily lives. Now, looking to threats on the horizon, what progress has been made, and what work is left to be done? Join Carnegie and the U.S. Cyberspace Solarium Commission for a conversation featuring leaders from the US government, and the energy and financial services sectors as they asses what comes next in securing domestic and global infrastructure in cyberspace.

If you're interested in or involved with Church Safety Security, you will want to attend this Free, open event and can learn more about Faith Based Safety Security Coalition and Round Table events. provided by FBSSC.

View Video

Training | InfraGard National

September 29 @ 9:00 am - 1:00 pm PST

Insider Threat Awareness and Best Practices

This course features a special introduction and briefing from FBI Special Agent Reginald Reyes, Counterintelligence Strategic Partnership Coordinator for FBI Los Angeles. This 4-hour introductory course is designed for corporations and critical infrastructure and key resources (CIKR). This course is an introduction to how to best assess the needs of your organization, and the general first steps to form an insider threat program. Discussions will center around building something with minimal or no budget. Definitions, scope, industry standards, best practices, factors to consider before you start, planning and implementations tips are included. Additionally, we will cover why there is no"one-size-fits-all" approach for insider threat programs, and why you need to factor in your organization's culture.

Register

This is an open-source product. Redistribution is encouraged.

View Virginia Fusion Center Homepage

Click Here

Observe Suspicious Activity?

Report Online

Virginia Shield Coalition

"Awareness Through Information Sharing"
