CIAware

Awareness Through Information Sharing

Incidents/Articles of Note:

- US Officials Expect Foreign Meddling to Last Past Election Day
- Virginia Transportation Board Cancels I-73 Effort; US 220 Upgrade May Be Alternative (VA)
- Virginia To Receive $35 Million To Replace Lead Pipes (VA)
- Climate Change, Aging Infrastructure, Human Decisions Feed Into Disasters Like Hurricane Helene, Says Expert (VA)
- Pentagon Confirms 'Incursions' of Unauthorized drones Over Air Force Base (VA)
- How Virginia's Tech Industry Supports National Security (VA)
- More Than $100,000 In Damage Caused To RTD Light Rail Lines By Copper Thieves (CO)
- Report: Iowa's Rural Bridges Are Most Deteriorated In The Country (IA)
- Dozens Of Thieves Raid Freight Train In Chicago In Broad Daylight (IL)
- East Tennessee Rail Network Devastated By Helene Could Take Months To Reopen (TN)
- Trucking, Law Enforcement Partner To Fight Human Trafficking
- US Hospitals Prep For Supply Chain Constraints In Wake Of Baxter International Plant Closure

- Tools and Resources -

Resource | DHS CISA

#Protect2024

For years, America?s adversaries have targeted U.S. elections as part of their efforts to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and decision making. We expect 2024 to be no different. U.S. elections remain an attractive target for both nation-states and cyber criminals. As we move into the 2024 election cycle, CISA and our partners in the federal government are positioned to support election officials and private sector election infrastructure partners in addressing the physical, cyber, and operational security risks they face. Election officials are the frontline defenders in securing the electoral process?we are proud to stand shoulder-to-shoulder with them in this critical mission.

View Resource

Resource | Joint Cybersecurity Advisory

Iranian Cyber Actors Compromises CI Organizations

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Communications Security Establishment Canada (CSE), Australian Federal Police (AFP), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint Cybersecurity Advisory to warn network defenders of Iranian cyber actors' use of brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including the healthcare and public health (HPH), government, information technology, engineering, and energy sectors. The actors likely aim to obtain credentials and information describing the victim's network that can then be sold to enable access to cybercriminals.

View Advisory

View Virginia Fusion Center Homepage

Click Here

Observe Suspicious Activity?

Report Online

Not a VFC Shield Member?

Join Today

Useful Links

	webversion	VFC Fusion Site
VFC Shield	Report SAR	Shield Homepage
Virginia Fusion Center 7700 Midlothian Turnpike N. Chesterfield, VA 23235	Email Coordinator	All Products

---