VFC Cyber Program
Cybersecurity 5x5

Date Published: OCT 01, 2026

(U) Emergency Services Sector Cybersecurity 5x5

(U//FOUO) Introduction: The VFC's Cybersecurity 5x5 is a concise summary that highlights five key insights alongside five opportunities for mitigation in a specific critical infrastructure sector. This product is intended to give leaders a quick snapshot of a sector's cybersecurity posture to provide awareness and inform decision-making.

(U) 5 Key Cyber Insights on Emergency Services

1. (U) Emergency services have seen a significant increase in cyber-attacks, noting a shift in cyber threat actors' behavior from stealing data to disrupting operations.
2. (U) Cyberattacks on emergency services typically target mission critical technology, including public safety radio, public safety answering points (PSAPs), geographic information systems (GIS), and computer-aided dispatch (CAD), affecting communication and downstream operations.
3. (U) Emergency services are increasingly being targeted because they present opportunities for widespread real-world disruption and are more likely to respond quickly to ransom demands.
4. (U) The most common tactics for initial access include social engineering, brute-force attacks, and exploitation of known vulnerabilities in legacy, unpatched, or unsecure IP-based systems and remote services.
5. (U) The most common attacks on emergency services observed by the VFC include ransomware, phishing, compromised systems, and distributed denial of service attacks (DDoS), including telephony DDoS.

(U) 5 Opportunities for Mitigation

1. (U) Clearly define and document mission essential functions, those systems or services that must continue to operate during an incident or outage, and ensure a backup plan is established for rerouting communication traffic through internal solutions or an external partner if necessary.
2. (U) Establish a documented patching process that is prioritized by mission essential functions and known exploited vulnerabilities.
3. (U) Maintain offline, encrypted backups of critical data and regularly test the availability and integrity of backups.
4. (U) Utilize network segmentation and VLAN isolation to prevent malicious actors from moving laterally across IT and communications systems.
5. (U) Remain vigilant against unusual emails, phone calls, or text messages seeking account access, changes to multi-factor authentication, or urgent requests to bypass IT policies and procedures.

This is UNCLASSIFIED//FOR OFFICIAL USE ONLY information protected by Virginia Code Section 52-48, unless otherwise noted. ***Further dissemination of this information outside of your organization is prohibited unless written approval is obtained from the VFC prior to dissemination****. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Pursuant to Virginia Code Section 52-48(D), anyone violating distribution restrictions may be prosecuted and may be prohibited from receiving future reports. Please contact the Virginia Fusion Center at (804) 674-2196 if you have any questions or need additional information.*