MITIGATIONS

CISA and FBI strongly encourages critical infrastructure organizations and other organizations that are either SATCOM network providers or customers to review and implement the following mitigations:

Mitigations for SATCOM Network Providers

- Put in place **additional monitoring at ingress and egress points** to SATCOM equipment to look for anomalous traffic, such as:
  - The presence of insecure remote access tools—such as Teletype Network Protocol (Telnet), File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Secure Copy Protocol (SCP), and Virtual Network Computing (VNC)—facilitating communications to and from SATCOM terminals.
  - Network traffic from SATCOM networks to other unexpected network segments.
  - Unauthorized use of local or backup accounts within SATCOM networks.
  - Unexpected SATCOM terminal to SATCOM terminal traffic.
  - Network traffic from the internet to closed group SATCOM networks.
  - Brute force login attempts over SATCOM network segments.
- See the Office of the Director of National Intelligence (ODNI) Annual Threat Assessment of the U.S. Intelligence Community, February 2022 for specific state-sponsored cyber threat activity relating to SATCOM networks.

Mitigations for SATCOM Network Providers and Customers

- **Use secure methods for authentication,** including multifactor authentication where possible, for all accounts used to access, manage, and/or administer SATCOM networks**.**
  - Use and enforce strong, complex passwords: Review password policies to ensure they align with the latest NIST guidelines.
  - **Do not use default credentials or weak passwords.**
  - Audit accounts and credentials: remove terminated or unnecessary accounts; change expired credentials.
- **Enforce principle of least privilege through authorization policies.** Minimize unnecessary privileges for identities. Consider privileges assigned to individual personnel accounts, as well as those assigned to non-personnel accounts (e.g., those assigned to software or systems). Account privileges should be clearly defined, narrowly scoped, and regularly audited against usage patterns.
- **Review trust relationships.** Review existing trust relationships with IT service providers. Threat actors are known to exploit trust relationships between providers and their customers to gain access to customer networks and data.
  - Remove unnecessary trust relationships.
  - Review contractual relationships with all service providers. Ensure contracts include appropriate provisions addressing security, such as those listed below, and that these provisions are appropriately leveraged:
    - Security controls the customer deems appropriate.