OPERATION Winter SHIELD

Securing Homeland Infrastructure by Enhancing Layered Defense

Objective: Operation Winter SHIELD distills the FBI's 10 most impactful actions organizations can take to improve resilience against cyber intrusions. These recommendations were developed with domestic and international partners and draw on recent investigations to reflect adversary behavior and defensive gaps.

Adopt phish-resistant authentication

Why: Many breaches start with stolen passwords. Phish-resistant methods make it significantly harder for attackers to gain access.

START NOW

- Prioritize administrators, executives, and other high-impact accounts.
- Deploy phish-resistant methods (FIDO2 compliant security keys or device-bound passkeys) for authentication, remote access, and critical systems.
- If authenticator apps are used, require number-matching and domain display; avoid push-only approvals.
- Eliminate SMS based multi-factor and disable legacy authentication methods.

Implement a risk-based vulnerability management program

Why: Adversaries often exploit known vulnerabilities that remain unaddressed due to a lack of ownership, an undefined mitigation process, and unclear deadlines for resolution.

START NOW

- Maintain a complete asset inventory with owners and business criticality.
- Set remediation timelines based on risk; critical systems should be measured in days, not months.
- Use authenticated internal scans to reflect actual configurations.
- Document exceptions with compensating controls and fixed completion dates.

Track and retire end-of-life technology on a defined schedule

Why: End-of-life systems no longer receive security updates and, as a result, are routinely targeted.

START NOW

- Maintain a rolling 12-month EOL forecast, reviewed quarterly with owners and procurement.
- Track EOL systems by product, owner, location, and retirement date.
- Replace or isolate EOL assets; if delays occur, apply compensating controls with firm decommission dates.

Manage third-party risk

Why: An organization's security extends only as far as its least-protected vendor with network or data access. Adversaries often exploit these gaps to bypass stronger defenses.

START NOW

- Maintain a single list of third parties with access or data-handling responsibilities and named owners.
- Require strong authentication, least-privilege access, and monitored gateways where feasible.
- Audit for and disable unused accounts.
- Contractually require rapid breach notification, encryption, and annual control verification.
- Revoke access and confirm data disposition upon contract change or termination.

Protect security logs and preserve them for an appropriate time

Why: Reliable, preserved logs are essential for detection, response, and attribution. Adversaries often attempt to erase them.

START NOW

- Centralize authentication, email, endpoint, network, DNS, remote access, and cloud audit logs in a SIEM or centralized logging platform; export daily to protected, immutable storage.
- Retain logs based on legal and response needs (12 months is a common baseline).
- Synchronize system clocks and validate retention.
- To identify gaps in log centralization and retention, conduct quarterly exercise to review logs of activity for a single user and/or server.

FBICYBER

OPERATION Winter SHIELD

Securing Homeland Infrastructure by Enhancing Layered Defense

Maintain offline, immutable backups and test restoration

Why: Backups are routinely targeted early in intrusions; resilience depends on isolation and tested recovery.

START NOW

- Follow the 3-2-1 backup rule: maintain at least three copies of critical data on two different media types, with one stored offline and immutable.
- Secure backup platforms with strong authentication, separate admin accounts, and consoles limited to secured devices.
- Define recovery requirements, including configurations and identity systems.
- Test restorations regularly, measure recovery time, and remediate gaps.

Identify, inventory, and protect internet-facing systems and services

Why: Unnecessary exposure creates low-effort entry points for attackers.

START NOW

- Maintain a concise list of all internet-reachable systems with owners.
- Remove unnecessary exposure; require authenticated gateways for what remains.
- Disable direct internet-facing remote desktop; use brokered access instead.
- Regularly scan public IP space to detect new exposures.

Strengthen email authentication and malicious content protections

Why: Email remains a favored initial access vector for intrusions and fraud.

START NOW

- Publish and enforce DMARC, SPF, and DKIM for all sending domains; align third-party senders.
- Progress DMARC policy from monitoring to quarantine to reject as alignment matures.
- Quarantine high-risk attachments, block internet-sourced macros, and sandbox suspicious files.
- Enable time-of-click link protection and restrict automatic external forwarding.

Reduce administrator privileges

Why: Broad, persistent administrative access enables rapid escalation when credentials are compromised.

START NOW

- Minimize the number of administrator accounts and administrative group memberships to only those necessary.
- Those granted administrator access should only use those privileges when necessary, and use a standard account at all other times
- Require just-in-time admin access from secured devices using separate admin accounts.
- Restrict where administrator logins are permitted and block use on standard workstations.
- Monitor and alert on privilege changes and new admin accounts.
- Remove local admin rights from user devices, approving exceptions with expiration dates.

Exercise your incident response plan with stakeholders

Why: Practiced organizations respond faster, contain more effectively, and reduce impact.

START NOW

- Maintain a concise incident response playbook defining roles, decision authority, isolation actions, and evidence preservation.
- Conduct a focused 60-minute tabletop exercise quarterly with technical, legal, communications, operations, and leadership teams.
- Include law enforcement contacts in your incident response plan such as your local FBI field office to enable rapid coordination.