

TSA SD Pipeline-2021-02G

The Coverage Map

18
clauses

7 clauses directly addressed by BlastShield™

8 clauses where BlastShield™ directly helps

3 clauses which BlastShield™ does **not** touch

Here is the **whole picture**, including the parts we do not cover.

The Change Most Vendors Missed: It Is No Longer a Checklist

The 2021-02 series began as a prescriptive mandate: implement this list. TSA has since revised it into a **performance-based framework**. You document how you achieve the required outcomes, TSA approves the plan, and you assess it every year.



The Assessment Clock

Section III.G.2.d Sets the Pace



At least one-third of the policies, procedures, measures, and capabilities in your TSA-approved Cybersecurity Implementation Plan must be assessed **every year**. One hundred percent over any three-year period. Section III.G.2.b adds a cybersecurity architecture design review at least once every two years, including verification and validation of network traffic and system log review.

Standing controls up once is the easy half.

The BlastShield™ Coverage Map

Directly Addresses	Supports	Provides Evidence
III.B.2.a Zone-to-zone controls	III.B.1 Documenting zones and connections	III.D.2.b Baseline deviation records
III.B.2.b Encrypted in transit	III.C.3 Least privilege, separation of duties	III.G.2.b Architecture design review
III.C.1.b Legacy assets, no password reset	III.C.4 Shared accounts	III.G.2.d The annual assessment third
III.C.2 Multi-factor authentication	III.D.3.b Log retention	IIV.C.2.e East-West and North-South records
Vendor Access Third-Party Sessions	BlastShield does not cover:	
III.D.4 Isolate ICS during an IT incident	III.C.5 Domain trust review Requires: Your own schedule and process	IIV.C.2.c Network and architecture diagrams Requires: Your existing network documentation
III.E.3 Compensating controls, unpatchable assets	III.D.1 Malicious email, IPs, domains, code, C2 Requires: Email security, web filtering, endpoint and network detection	

Three Clauses Worth Knowing

The Three That Change a Conversation

III.E.3 Where patching would cause severe degradation of operational capability, the directive requires you to describe additional mitigations instead. The regulation contemplates compensating controls for unpatchable assets. An asset that does not answer an unauthorized scan is one of them.	III.D.4 and III.F.1.d Two separate clauses require the capability to isolate OT when an IT incident threatens it. Isolation by policy change, not by pulling cable. The change is logged.	III.C.1.b Components that will not have passwords reset on schedule need documented mitigations. Passwordless access removes the need for credentials rather than managing them.
---	---	--

What the Assessor Gets

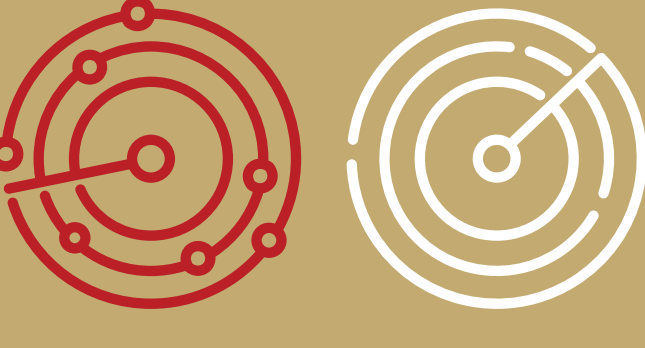
Evidence, Not Assertions

 Both permitted and denied access attempts , with identity and timestamp	 Configuration changes , logged	 Policy configuration , exportable and reapplicable
 Vendor sessions , recorded in full	 Four export paths: local, API, syslog, FTP in CSV	

Retention is configurable, so it can align with your assessment cycle rather than **the other way around**.

The Test

Twenty Minutes, One Artifact



Side-by-side port scans, unprotected versus protected, produce a dated artifact for **Section III.G.2.c**, and it is the fastest way to establish whether any of this holds in your environment.

BlastWave publishes compliance mappings. **BlastWave is not certified or accredited** to any regulatory framework, and no vendor product confers compliance on an operator. This mapping supports, but does not replace, an operator's own implementation plan, assessment plan, and formal determination by TSA.