

INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

CRITICAL INFRASTRUCTURE PROTECTION
HSI Industrial Skills – Reliability Matters

Key Observations

Local Risk of Low Impact Assets

– Although individual low-impact BES Cyber Systems usually present a minimal risk, their compromise can cause local problems or allow access for larger attacks.



CIP-003 R2 Compliance

– The majority of low impact cybersecurity requirements are found in CIP-003 R2. Noncompliance with this standard has been rising since 2017.



EXAMPLE 1 Misunderstanding Obligations

Improper or limited training of personnel responsible for completing requirements

Low impact sites experiencing changeover in ownership leadership, operations management, and/or compliance oversight

EXAMPLE 2 Cyber Environment Understanding

Lack of understanding of the environment results in incomplete network diagrams and inaccurate or missing system configuration details

Poor access management fails to secure connections and third-party integrations

EXAMPLE 3 TCA Plan Implementation

Documented plan exists, but documentation for TCA scans is missing

Inability to track or manage Transient Cyber Assets



Suggestions for Improvement

Know what technology is in your environment and how it operates

Ensure you understand and protect the configuration of your technology

Provide and document consistent training on security practices and objectives

Maintain open channels between staff and leadership for identifying and mitigating vulnerabilities

Clearly outline roles and responsibilities, including third-party involvement with tools like a Roles and Responsibilities matrix

Regularly check that your program is effectively implemented and achieving desired security results utilizing internal controls and scheduled self-evaluations

