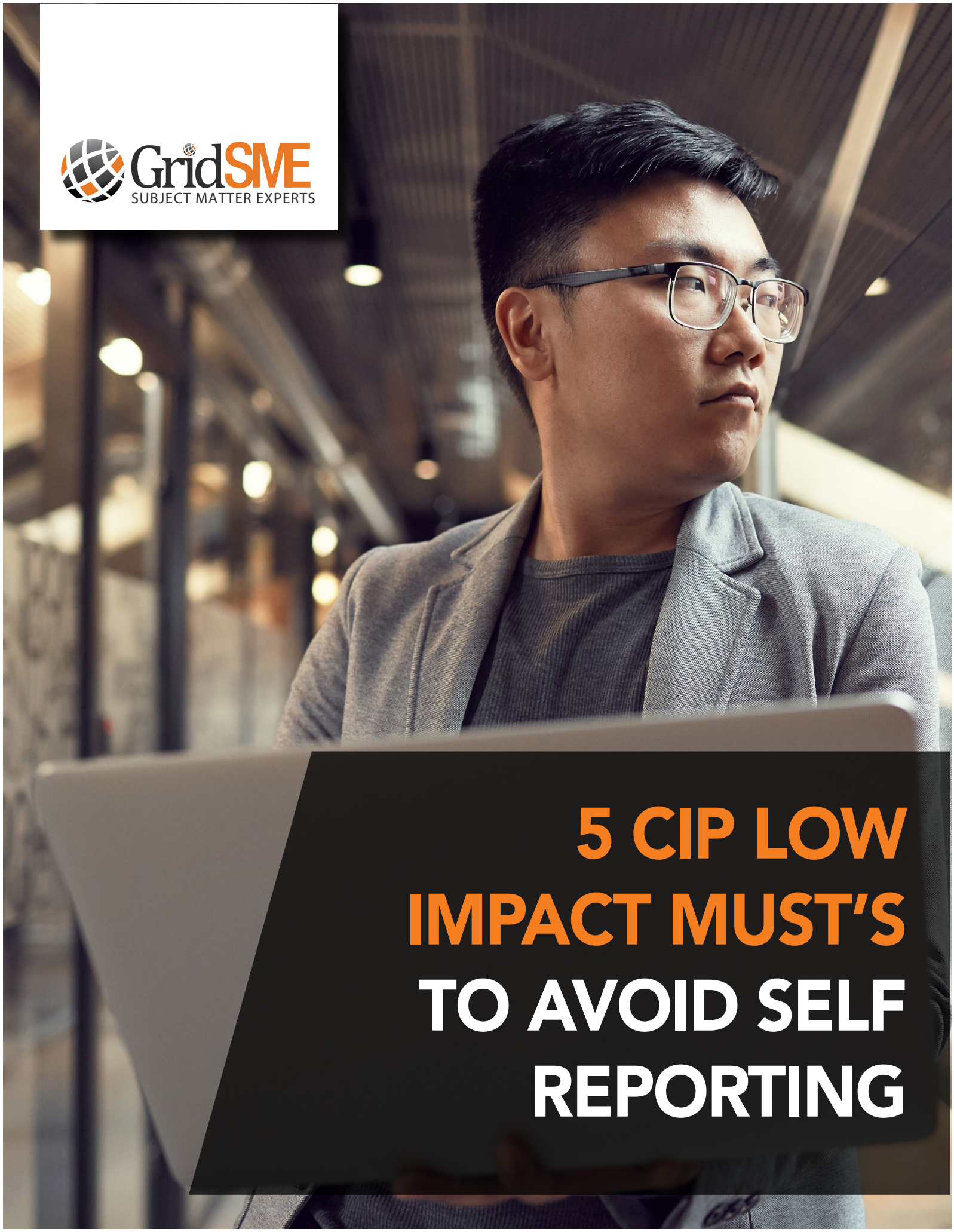
GridSME
SUBJECT MATTER EXPERTS
5 CIP LOW IMPACT MUST'S TO AVOID SELF REPORTING

While new CIP standards seem to be coming out all the time, CIP-003-7 is particularly noteworthy as it is the first time that low impact facilities will need to implement ongoing technical controls in the field. Below is a list of five (5) "to do's" and "to have's" to avoid self-reporting for non-compliance

1. Obtain CIP Senior Manager review and approval via signature of your *CIP Low Impact Cyber Security Policy and CIP Exceptional Circumstance Plan.*

2. Obtain and retain evidence for physical security controls.

3. Obtain and retain evidence for electronic access controls.

4. Obtain and retain evidence for Transient Cyber Assets (TCA) and Removable Media (RM) controls.

5. Communicate, coordinate, and train (as needed) personnel on the new requirements.

As of 1/1/20, in addition to existing CIP-003-6 requirements, each registered entity with low impact BES Cyber Systems will need to:

- Demonstrate proof of implementation of documented physical security controls;
- Demonstrate proof of implementation of documented electronic access controls;
- Demonstrate proof of implementation of Transient Cyber Assets (TCA) and Removable Media (RM) plans; and
- Have a documented CIP Exceptional Circumstance plan.

Additionally, auditors from the Regional Entities have made it clear that they expect Responsible Entities to self report each and every time their Transient Cyber Asset and Removable Media plan is not followed. The same goes for physical and electronic access control procedures.

What you need to do

While we have been working closely with our clients for over a year to prepare, there may still be confusion on just how serious the need is to complete the work required to avoid self-reports. For those of you that we do not provide Managed Security Services to, we need you to reach out to your GOP and O&M Providers and urge that they provide all items we've requested in order to help you be compliant by the due date.

1. The CIP Senior Manager must approve the new CIP Low Impact Cyber Security Policy (and CIP Exceptional Circumstance plans, if separate from the policy).

Evidence includes but is not limited to:
a. Signed, dated, and versioned policy(ies)

2. Physical security controls evidence must be generated and retained.

Evidence includes but is not limited to:
a. Physical security diagram showing the location of specific controls (e.g. access gates, video cameras, etc.).

b. If physical lock and key programs are used to control site access, O&M Providers needs to provide information about the key management program and provide evidence of implementation (e.g. key inventory, etc.).

c. If a visitor management program is part of the O&M site control, O&M Providers need to provide evidence of implementation (e.g. visitor logs, etc.)

3. Electronic Access Controls evidence must be generated and retained

Evidence includes but is not limited to:

a. Updated and accurate network diagram for the entire BES Cyber System(s), denoting all electronic access points (e.g. firewalls, modems, routers) and remote connections (e.g. VPNs, Internet traffic, etc.).

b. Firewall ruleset with all permitted inbound and outbound communications justified.

c. If dial-up access is present, evidence that authentication is enforced.

4. Transient Cyber Asset and Removable Media information and evidence must be generated and retained.

Evidence includes but is not limited to:

a. If entity-owned and managed TCA's are allowed, provide details and evidence of continuous management and monitoring (e.g. anti-virus policies, patch management methodologies, etc.). This evidence must also identify the devices that are authorized TCA's and the controls applied.

b. If 3rd party-owned and managed TCA's are allowed, provide evidence of verification checks to ensure those devices have the required controls implemented (e.g. clean anti-virus scan, up-to-date patches, etc.). Provide evidence that there is a process to have these verification checks performed, prior to allowing the TCA to connect to the BES Cyber System.

c. If RM is allowed, provide evidence that there are technical means to scan RM for viruses using a device outside of the BES Cyber System, prior to allowing the RM to connect to the BES Cyber System.

d. Provide information on controls in place to determine if the TCA or RM verification processes are ever bypassed, whether inadvertently or maliciously.

5. Communicate, coordinate, and train personnel on the new requirements.

Evidence includes but is not limited to:

a. Particularly over-communicate the physical and TCA/RM plans and processes as they rely most heavily on field personnel and impact 3rd party vendors and contractors the most. As a result, they are the most likely requirements to be inadvertently violated.

b. As with all new compliance requirements, frequent check-ins with personnel who are affected by the new requirements should occur. In the beginning, daily or weekly check-ins may be warranted, moving to monthly or quarterly check-ins once personnel are more comfortable with the processes and requirements.

c. Be sure that personnel know to report break-downs in process to the CIP Senior Manager so that the situation can be appropriately addressed (and self-reported, if deemed appropriate).

GridSME
SUBJECT MATTER EXPERTS

DO YOU NEED HELP SECURING YOUR FACILITIES & PROTECTING YOUR INVESTMENT?

SCHEDULE A CALL

OUR SERVICES

- **MANAGED SECURITY SERVICES**
- **MANAGED SCADA SERVICES**
- **MANAGED NETWORK OPERATIONS**
- **DESIGN, CONFIGURATION, & ASSESSMENT**