Executive Summary

If cyber security could be guaranteed by standards alone, America’s power grid would have little to fear.

The North American Electric Reliability Corporation’s (NERC) team drafting its standards for Critical Infrastructure Protection (CIP) first convened in 2008; it has since published four versions, with the latest to be implemented in 2014. NERC CIP version 5, meanwhile, is well underway.

There was some logic in this approach. The decision to publish early reflected an understandable desire to put basic standards in place to protect the grid while solutions were sought for the more complex challenges posed in meeting the requirements of the Federal Energy Regulatory Commission (FERC). But it also has its weaknesses, with the constant revisions to the standard undoubtedly contributing to utility executives’ reluctance to commit to early action.

Even now, with version 4 receiving approval from FERC in April, and with increasing clarity on the principal changes in version 5, many are waiting until the standards are formally implemented before taking action. Given the uncertainty in the drafting process—with real speculation for a time that version 4 would never actually be implemented because version 5 was being developed in tandem—that is not surprising. Executives tend to struggle to see the return on investment in cyber security in any case, since it is difficult to value preventative action.

However, in reality there’s little to be gained from a delay in addressing the challenges NERC CIP presents, and, potentially, much to be lost.
Table of Contents

A Broader View ......................................................................................................................... 3
Time for Change.............................................................................................................................. 3
The Compliant Culture .................................................................................................................. 4
A Broader View
For a start, whatever uncertainty there has been in the drafting, little now remains. The most important changes are now very clear. Principle among them is the standards’ scope.

By far the most significant criticism of the CIP standards to date was their failure to address the majority of the grid. Earlier versions of the standards left it to power companies to determine whether their facilities constituted “critical cyber assets”, qualifying them for inclusion in the program. In doing so, the NERC team unintentionally, but effectively, granted the majority an opt-out. Most simply declared their facilities were not critical, either because the loss of the asset would not significantly impact the bulk electric system (since removal of very few assets on their own would have a catastrophic impact on overall electricity supply); or—more weakly—on the basis that a facility could be safely taken offline and its contribution removed from the grid.

Such exemptions were clearly not the intention of the drafters of the CIP standards, for whom the aim was to increase the overall stability and reliability of the grid. Nevertheless, they have been extremely effective in limiting its impact. A survey by the Western Electricity Coordinating Council, one of the country’s three major grids, showed just 17 per cent of its facilities participating—the implication being that North America could function with fewer than four in every five of its electric assets.

This absurdity is addressed squarely in CIP version 4, which focuses almost entirely on establishing “bright-line criteria” to determine criticality—and thus inclusion in the NERC CIP program. These are based on objective measures such as facilities’ voltage, generation capacity and inter-connect numbers. Identification of critical assets is therefore no longer left to the “responsible entity”—the asset owner—which should massively increase the number of facilities drawn into the standards.

Moreover, whatever tweaks there may be to the details of version 5, its approach is also becoming clear. Within eight to twelve months, it’s likely there will be something close to a final version that should at last fully address the FERC’s Order 706 setting out what it requires from the standards. And it looks very likely that it will expand the scope of the standards even further.

Significantly, version 5 introduces different levels of compliance, with a baseline set of security practices for all facilities and cyber assets affecting BES reliability (again, determined objectively), and a higher level of control for more critical assets. This will see a significant expansion in the number of assets and facilities that must comply with the CIP in some way. Under this, it will be increasingly hard for companies to argue that their assets are not vulnerable to at least inadvertent, non-malicious threats to network security (by far the more realistic threat compared to targeted attacks); and impossible in the vast majority of cases to argue that such vulnerabilities have no impact on BES reliability. In fact, the drafting team is moving away entirely from a site by site discussion of grid impact towards a presumption that all assets are of some level of importance and therefore need protection.

Whatever the differences, however, in both versions 4 and 5 the most important result is the same: the loophole that allowed many facilities to avoid compliance with the standards will be closed. Almost every NERC entity will therefore see more of their cyber assets having to comply—and in many cases, a lot more.

Time for Change
Even allowing for this, some continue to take consolation from the fact that facilities will have two years from the date of adoption to comply with the standards. Again, however, it’s false comfort.

First, any savings from delay will be more than outweighed by the difficulties in securing the expertise to help implement a compliance program closer to the deadline.

The number of operators excusing themselves from the standards up to now means that once CIP V4 is implemented, demand for support in implementing a compliant program will rocket, putting pressure on costs. In fact, there must be questions of the capacity in the industry to meet this since the combination of IT expertise and process control experience required for cyber security strategies is already rare. At best, by leaving it to the eleventh hour, operators risk paying significantly higher costs in securing the appropriate skills sets to implement compliant programs; at worst, they risk finding themselves with little choice but to take on support with questionable skills or experience, opening the risk to outages, slowdowns or regulatory action in the process.
There are also two further factors facility owners should bear in mind. The first is their preparedness to implement a cyber security program.

The most basic starting point for designing, installing and configuring a CIP program is an inventory of cyber assets. Operators must know the operating systems and IP addresses of the assets on their networks; what applications are running on each and the processes being controlled; the local arrangement of those assets—where they lie on the network, and their physical location onsite. Without this information about their assets, it is impossible for operators to determine their criticality or secure them. In reality, however, a good number of entities simply don’t know what equipment they have plugged in.

For those with larger networks, with dozens of generation sites, remedying that is a huge undertaking on its own, and it’s far from clear how much thought has been given to the resources needed to address it. Planning long-term, compliance for such operators is achievable, and they can build in this work to regular day-to-day operations, developing a full inventory over time. Left until later, however, those with multiple sites will find a two-year window to implement a compliance program from scratch is far from generous—and all the more bearing in mind the second factor facility owners should consider: the end point critical asset owners have to get to.

The Compliant Culture

There are, in fact, two phases in working towards CIP compliance.

The first is to design, install and configure a cyber security program with effective controls. This is a substantial endeavor, and parts of any program will need significant lead times. For example, even with the resources available to implement physical security systems, such as swipe cards, cameras and data collection points to control access to critical equipment, the periods required to negotiate contracts and the scope of on-site work in larger facilities is likely to push a two-year implementation deadline. Added to that, many facilities will need to fit that work around periods or seasons of peak demand, leaving relatively narrow windows to do it.

Arguably, however, the greater challenge is longer-term—the second phase of compliance. Indeed, the case for delaying work to implement CIP programs by a matter of months to take full advantage of the two-year lead-in is even weaker when one considers that the program will be running for decades to come. Compliance with NERC CIP is not an isolated event; it is a new way of working.

Utility companies must put in place not only the systems and procedures to ensure the robustness and security of their critical assets, but also the training, continual improvement programs, communication and regular review to ensure sustained compliance. Unless employees are familiar with and support the security program’s concepts and controls, it will not be implemented successfully and the desired level of security will not be achieved.

Furthermore, power companies also need to prove compliance to outside auditors: procedural documents addressing how the organization addresses the specific CIP standards; forms providing the evidence of compliance with those procedures; and accompanying technical documentation detailing the network infrastructure, user accounts and security controls in place. Again, personnel must fully buy in to the program for this to be achieved. If compliance is to demonstrate convincingly, the program’s procedural and policy objectives must be embedded into employees’ day-to-day tasks.

Here, too, it’s unclear how much thought businesses that are waiting until the ink dries on the standards have put into the resources and time needed, much less how they will develop and ingrain the cultural change within their plants that compliance with the standards implies.

The obvious desire of the regulators is to ensure cyber security is entrenched in the grid’s process control in the same way as the culture of safety has been established—a process that took decades and continues to be a daily challenge. Regulators will not be satisfied with operators’ efforts and won’t rest until that’s the case. Given that, it is increasingly hard to argue that it’s too soon to make a start.

Honeywell has one of the largest collections of NERC experienced cyber security experts in the industry. Our depth and breadth of history in the assessment, remediation and ongoing management of a NERC CIP program across a host of control system vendors means we can help you get started today. From front end baseline inventories to gap analysis, program planning and the selection, implementation and management of security technologies, we provide flexible, scalable, cost-effective solutions for your organization.
For More Information
Learn more about how Honeywell's Industrial IT Solutions and how they can enhance the security of your operations, visit our website www.honeywellprocess.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com