NERC CIP VERSION 5

TOP 10 CHALLENGES

With suggested solutions

401 Congress Avenue, Suite 1540
Austin, TX 78791
Phone: 512-687-6224
E-Mail: chumphreys@theanfieldgroup.com Web: www.theanfieldgroup.com

Introduction

Last year, we issued a poster titled “Top 10 NERC CIP Version 5 Transitional Challenges.” That poster proved to be extremely successful in getting people to think about the compliance challenges posed by NERC CIP Version 5. As a follow up, we created this whitepaper to provide more details around each transitional challenge and the technological solutions available to address them. Here at The Anfield Group, we have always prided ourselves on being industry thought leaders in holistic security and compliance program development. In addition, I’m confident that most of our colleagues and clients agree that when it comes to understanding the technologies needed to sustain and automate compliance as a byproduct of operational and security best practices, The Anfield Group’s knowledge is unmatched in the industry.

As the industry begins to implement NERC CIP Version 5 programs ahead of the April 2016 compliance date, The Anfield Group wants to make sure the industry is equipped with the proper technologies to successfully manage its compliance obligations. Plus, we intend to continually promote the holistic strategy of operational and security efficiency. The manual execution of a NERC CIP Version 5 Compliance program is neither sustainable nor efficient for the industry.

Lastly, while technology is essential to security sustainability and compliance, it has a proper place in the maturity of a utility. If technology is viewed as a “magic bullet” and improperly implemented before mature processes, controls and requirements are defined and tested, that technology will fail. It is our hope that through this whitepaper, the transitional challenges from a process and control perspective combined with the technology recommendations will encourage NERC-registered entities to examine their own programs and identify what technologies they may currently have, what gaps exist from both a process/control perspective and a solutions perspective to sufficiently establish the foundation for a sustainable NERC CIP Program.

Chris Humphreys

CEO/Director

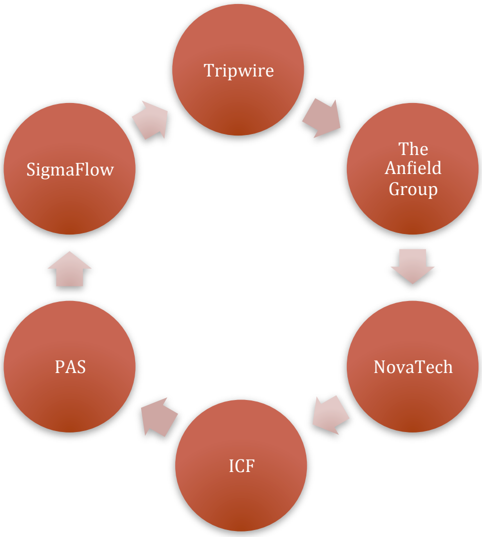
The Anfield Group

NERC Alliance Network

The Anfield Group is an active member of the Tripwire NERC Alliance Network (NAN). Our role within the alliance is to provide the NERC Compliance and Security Program Architecture and regulatory perspectives where the technologies represented within the alliance serve as integral components to lowering overall compliance and security risks. With The Anfield Group providing the compliance process, security controls, and regulatory expertise and NAN Solutions members providing the toolsets, the collective NERC Alliance Network provides the industry's only end-to-end solution set for holistically addressing the NERC CIP Regulatory framework.

SigmaFlow, **Novatech**, and **Tripwire** are NAN members who have contributed content to this whitepaper. **Contact information** for each is on page 26.

Created in 2014, Tripwire's NERC Alliance Network collaboratively brings companies together who offer high-quality energy sector and NERC-focused solutions, services, and technologies. These offerings automate and simplify NERC CIP compliance and technology challenges in the power industry. Alliance Network goals include: Collaboration; Education; Marketing and Promotions; Lead Sharing; and Proof of Concepts. For details, including information on joining the network, click here.



While The Anfield Group (TAG) is a member of the Tripwire NAN, TAG does have extensive knowledge with external technology partners within the verticals of Governance Risk and Compliance (GRC), Regulation Management, Security Event and Incident Management (SEIM), Identity and Access Management (IDM), Network Simulation and Visualization, Firewalls and Network Devices, and Physical and Logical authentication technologies.

CHALLENGE 1: BES Cyber System Identification

NERC CIP Version 3

Under NERC CIP Version 3, CIP-002-3 required entities to develop a Risk-Based Assessment Methodology (RBAM) for identifying Critical Assets (CA) and corresponding individual Critical Cyber Assets (CCA). The Entity was only required to consider certain asset types with some very subjective and non-defined criteria for determining if the entity did or did not have NERC Critical Assets and corresponding Critical Cyber Assets.

NERC CIP Version 5

With CIP-002-5, Version 3's RBAM approach for identifying CA and CCA is discontinued. In its place, entities must utilize the BES Cyber System Identification requirements to identify the entire system. Then, classify CA into Low, Medium and High categories of criticality. These categories of criticality are defined with much more granularity than Version 3 in CIP-002-5's Attachment 1. Varying levels of protection are required for each category. CCA are not to be defined individually. Instead, they are to be defined as components of a BES Cyber System.

Consequences

Version 5's new approach to determining criticality means that some entities that were not required to be NERC CIP compliant under Version 3 may very well find they are no longer exempt under Version 5. As a result, they will be required to develop and implement a NERC CIP Compliance Program that is far beyond the minimal requirements of CIP-002 and CIP-003.

Additionally, entities that had a full CIP-002 through CIP-009 program under Version 3 will find that process control enhancements must be made as a result of the more clearly defined criteria in Attachment 1 of CIP-002-5.

Suggested Strategies:

A foundational technology that can be utilized for all NERC Reliability Standards, including CIP-002-5, is Governance Risk and Compliance (GRC). GRC allows for the automation and enforcement of process controls and policy elements combined with document management functionality. At its most advanced, there are enterprise-wide GRC solutions being deployed that directly integrate to third-party systems and applications along with any home-grown technologies that can actually associate and aggregate output data from those systems and tie it to a compliance requirement or process control. At its most basic, GRC can offer extremely user-friendly workflow interfaces, process tracking, and document management. When selecting a GRC technology, it is crucial to scale based on extremely well defined requirements to justify how robust a GRC deployment will be needed at a utility. Either way, the end state should be focused on GRC enabling overall operational/security efficiencies where compliance outputs are a natural byproduct of properly implemented tools and validated process controls.

In the case of CIP-002-5, being able to automate and track the BES Cyber System Identification process entities will be required to have implemented is a key use-case for exploring GRC. The, at least, annual requirement of the execution of the BES Cyber System Identification Process and the need to discover and manage BES Cyber Assets within the environment shows that manual process execution is neither efficient or sustainable. By combining an enterprise-wide GRC deployment or a very-focused NERC-specific GRC equivalent (i.e. SigmaFlow) with the asset management and identification of Tripwire's IP 360 suite, an organization can lower their risk of non-compliance and ensure consistency in process execution while optimizing staff and resources through automation.

Suggested Solutions:

SIGMAFLOW®

The SigmaFlow Compliance Manager solution provides a preconfigured model with workflow procedures for assessing and reviewing: BES Assets, Systems (BROS to determine BES Cyber Systems), and Cyber Assets. The SigmaFlow model includes automatic Cyber Asset Classification (BCA, PCA, EACMS, PACS) and has the “High Water Mark” functionality built into the solution for mixed-mode ESPs. In addition, the solution is preconfigured to show applicable Requirements for each BES Cyber System and Cyber Asset managed by the solution to ensure Utilities understand the NERC CIP Requirements that apply to each BES Cyber System and each Cyber Asset in an ESP of High or Medium Impact Rating. Finally, the solution provides the means to review supporting compliance evidence for all Requirements applicable to each BES Cyber System and Cyber Asset and to identify all applicable Requirements where evidence does not exist.

tripwire CONFIDENCE: SECURED

Tripwire IP360 combined with professional services use of Tripwire discovery tools can help identify and track the critical cyber assets that are in scope. Tripwire IP360 can also discover all assets in assigned IP scope using TCP and UDP protocols. Discovery of all assets allows for further classification and integration.

Tripwire Enterprise can monitor systems to determine what software, services, protocols, and ports are in use. Together, both products contribute to insights leading to a more complete inventory from which to determine what assets should be considered BES CCA and at what level (high, medium, low).

CHALLENGE 2: Inbound and Outbound Network Access Permissions

NERC CIP Version 3

Version 3 of CIP-005 did not specify the inclusion of inbound and outbound access permissions in the requirements. R2.1 of CIP-005-3 did require a “deny by default” access model. Although it could be inferred that R2.1 required the inclusion of inbound and outbound access permissions, it was not specifically included in the requirement.

NERC CIP Version 5

CIP-005-5 R1.3 now requires inbound and outbound access permissions, granting of the access, and by default, the denial of all other access.

Consequences:

While it was common under Version 3 to see a firewall rule set or access control list as an output to demonstrate compliance, documenting the reasoning for each type of network access permission was not required. However, under CIP Version 5, management of firewall rules and/or access control lists must have documented justifications for each rule or access type.

Suggested Strategies:

Hardening Firewall Rules and Access Control Lists (ACLs) are the essential technical controls to addressing NERC CIP-005-5 R1.3. With that hardening, an organization must also have the ability to manage and enforce ACLs and Firewall rules. Technologies such as Cyber Security Gateways (i.e. NovaTech Orion) can establish secure encrypted, connections to substation assets along with monitoring all inbound and outbound user activity with active Firewall rule enforcement. Security tools such as Tripwire can support the monitoring of both inbound and outbound traffic through the enforcement of approved ports and services and can detect for variances against the established approvals. With a GRC solution (i.e SigmaFlow) on the enterprise that can directly integrate to the security tools and gateways, the outputs from tools like NovaTech and Tripwire can be aggregated against an establish process or control.

Suggested Solutions:

NovaTech

A built-in stateful firewall restricts access to NovaTech's OrionLX Cyber Security Gateway in the substation. The firm's Connection and Identity Manager assigns each user privileges that restrict access to specific substation assets and how access should be made (SSH, HTTPS, etc.). Permitted tasks are also restricted ("view only," "change time frame," etc. Security is further enhanced by strong, centrally-managed passwords.

tripwire

CONFIDENCE: SECURED

Both Tripwire IP360 and Tripwire Enterprise monitor ports and services and compare current state against a tailored set of customer-specific approved port and services. Alerts are issued when monitoring detects a variance. Tripwire Enterprise confirms known good-sets of services, ports, and protocols. Tripwire also detects whether removable media has been connected to a monitored system, providing timely alerting to potential violations.

SIGMAFLOW

The SigmaFlow Compliance Manager solution collects the Access Rules typically contained within Firewall rule-sets and control lists. For reporting, these rules are collected either as documents or as data. Because this information is retained in SigmaFlow as data rather than as one or more documents, the SigmaFlow solution can be used to review, approve, modify and query this information at any level.

CHALLENGE 3: Detecting Malicious Communications

NERC CIP Version 3

Not required in NERC CIP Version 3

NERC CIP Version 5

CIP-005-5 R1.5 requires that all Electronic Access Points for medium to high-impact BES Cyber Systems must have "one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications." Examples of evidence showing this requirement has been met include documentation of application layer firewall and/or intrusion detection system (IDS) implementations.

Consequences:

Despite the lack of any previous requirement to do so, many utilities implemented IDS simply out of a desire to achieve security best practices. For utilities that find they are now required to meet the requirements of NERC CIP Version 5, the now required implementation of an IDS or application layer firewalls may pose a significant challenge.

Suggested Strategies:

Intrusion Detection Systems can monitor and analyze user and system activity, audit system configurations and vulnerabilities, and assess critical system data file integrity. From a security best practice perspective, it's easy to see why and IDS would be implemented. IDS can also detect data alterations, system configuration errors, and detect attacks.

Suggested Solutions:

tripwire
CONFIDENCE: SECURED

Tripwire scans for anti-virus and malware products installed through tailored change auditing rules. Logs are monitored to find specific malware events and the Tripwire operator examines the device for incident information. Tripwire's monitoring detects the introduction of unapproved/unauthorized files on a given system.

SIGMAFLOW®

SigmaFlow Compliance Manager includes both Malware and Anti-Virus checks in the Security Controls it manages. With Security Controls integration, the SigmaFlow solution can validate on a periodic basis (ex. – daily) these Security Controls for all CIP Cyber Assets. In addition, the SigmaFlow solution manages the evidence that describes the methods used to detect malicious communications, and records, tracks, and uses workflow to manage (and document) the response to the detected malicious communications.

NovaTech®

In the substation, the OrionLX Cyber Security Gateway monitors login attempts of all authorized and unauthorized users, as well as the type of login (remote, local, root, etc.)

CHALLENGE 4: Use of Intermediate System for Remote Access

NERC CIP Version 3

Not required in NERC CIP Version 3

NERC CIP Version 5

CIP-005-5 R2.1 requires the inclusion of an Intermediate System for Interactive Remote Access so that “the Cyber Asset initiating the Interactive Remote Access does not directly access an applicable Cyber Asset.” Instead of remotely accessing in and out of an Electronic Security Perimeter (ESP), there now must be an intermediary (i.e. VM instance/jump host) between the external paths into the ESP. In addition, R2.3 and R2.4 of CIP-005-5 require that the Intermediate System must be encrypted with multi-factor authentication.

Consequences:

Although a known security best practice, the lack of required compliance has resulted in intermediate systems being used only sparingly throughout the industry. As a result, for most utilities the implementation of an Intermediate System for Interactive Remote Access will be an additional and potentially perplexing challenge.

Suggested Strategies:

Deciding which Intermediate System technology to deploy all comes down to a question of scalability. From a NERC perspective, they strongly discourage remote access in and out of an ESP all together. However they understand that it is neither efficient nor practical to enforce a zero tolerance for remote access. To compromise, the NERC SDT has added the Intermediate System requirement to Version 5. When examining technologies for Intermediate Systems it is important that the entity define both short term and long term requirements with respect to remote access authorization.

Suggested Solutions:

Where not generated internally within the solution, the SigmaFlow solution is used to collect evidentiary documents and associate them to the appropriate Requirements for use with RSAWS, Audit Packages, or as additional supporting evidence that may be desired for internal review or additional evidence requests during a formal CIP audit.

When accessing remote substation assets, The NovaTech Connection and Identity Manager serves as this Intermediate System.

Tripwire tracks settings associated with authenticated access control for remote use. Tripwire validates and monitors security settings and configurations made to ensure strong authentication by external interactive user. Tripwire's ability to know which ports, protocols, and services are approved and within baseline uses helps track changes when they occur.

CHALLENGE 5: Protection of Unnecessary Physical Input/Output Ports

NERC CIP Version 3

Not required in NERC CIP Version 3

NERC CIP Version 5

CIP-007-5 R1.2 improves security by eliminating unnecessary physical input/output ports. This can be done physically with port locks or signage or logically through system configuration in accordance with the Measures Section of the requirement.

Consequences:

Compliance with this requirement requires: 1.identification of all unnecessary physical input/output ports; 2.disabling of these ports; and providing documentation confirming that the disabling has been achieved.

Suggested Strategies:

Implementation of physical port locks to satisfy this requirement is becoming more and more common. Additionally, the capacity to track physical port openings and closures without the proper tools will be exceedingly challenging. Validated process controls being enforced through a GRC solution that can identify all physical ports serves as a complimentary solution for managing the protection of physical ports.

Suggested Solutions:

SIGMAFLOW®

Where not generated internally within the solution, the SigmaFlow solution is used to collect evidentiary documents and associate them to the appropriate Requirements for use with RSAWS, Audit Packages, or as additional supporting evidence that may be desired for internal review or additional evidence requests during a formal CIP audit.

NovaTech®

The OrionLX Cybersecurity Gateway in the substation is shipped with all unnecessary ports closed. Unused physical ports can be removed or blocked.

CHALLENGE 6: Security Patch Implementation Mitigation Plans

NERC CIP Version 3

Entities were required to document compensating or mitigating measures taken as a result of not installing security patches.

NERC CIP Version 5

CIP-007-5 R2.3 introduces a mitigation plan component that must be implemented whenever a security patch is not installed within 35 days of the completion of a patch assessment. The plan must include details on how the vulnerabilities addressed by each security patch will be mitigated and the timeframe for completed the required mitigation.

Consequences:

This requirement is a significant change from Version 3. The detailed formalization of a mitigation plan requires entities to complete the installation of issued security patches within a specified timeframe -- or implement a detailed mitigation plan.

Suggested Strategies:

Patch Management is traditionally achieved within the industry between a combination of subscription-based patch availability services and enterprise patch solutions. Due to the variety of system environments, patch management is often a very manual process even with certain tool sets. A well-documented Patch Management Program combined with a GRC platform that can integrate patch management notifications from disparate tool sets and automate the generation and monitoring of patch deployment schedules and mitigation plans will be the keys to successfully meeting the compliance requirements in CIP-007-5.

Suggested Solutions:

The SigmaFlow solution includes data collection and workflow for security patch assessment. The solution also includes Patch Management as part of the Asset Change Management workflow procedure, which includes (via integration) the ability to validate and produce evidence that security patches were successfully installed on all Cyber Assets included on a Patch Change Ticket. The SigmaFlow solution produces the evidence required for NERC CIP compliance for both the Patch Assessment and Asset Change Management workflow procedures automatically.

Tripwire isn’t a patch management tool. However, it identifies software versions and installed patches and compares current state against a tailored set of customer-specific approved software versions and patches. Alerts are issued when there is a variance on specific BCA's. Based on vendor recommendations, IP360’s vulnerability assessment capabilities identify any necessary patches that should be installed on a broad range of BCA systems. The vulnerability database is typically updated every week. Tripwire detects when patches are implemented and records this information for later review and analysis.

CHALLENGE 7: Baseline Configuration Management

NERC CIP Version 3

CIP-003-3 R6 is currently the only requirement that is specific to Change/Configuration Management. It requires a change management process but does not go to the level of granularity with regard to establishing and maintaining baseline configurations by device per CIP-010-1 in Version 5.

NERC CIP Version 5

Configuration management is one of the most expanded components of CIP Version 5. In fact, Version 5 introduces an entirely new Reliability Standard -- CIP-010-1 "Configuration Change Management and Vulnerability Assessments." CIP-010-1 requires a security baseline be established and maintained that includes OS level, commercially available or open source application software, custom software, logical network accessible ports and installed security patches. While this is a common security best practice to capture and maintain this type of data, there's never been a NERC requirement with this level of specificity with regards to security baselines.

Consequences:

Meeting the requirements of a completely new standard requires additional efforts, some of which can be labor and time intensive. For example, with R1.1 requiring the development of a baseline configuration arranged by asset or group of assets that include Operating System, commercially available or open-source application software, any custom software, logical network accessible ports and installed security patches having sufficient process and security controls established combined with the proper technologies to not only capture this data but also detect change deviations to the Baseline is going to be a relatively new endeavor for many NERC Registered Entities. Additional requirements in CIP-

010-1 address documentation, monitoring of deviations from established baselines and maintenance of baseline configurations.

Suggested Strategies:

Establishing formal security baselines for all BES Cyber Assets and being able to monitor and enforce those baselines is unsustainable via manual processes. Process controls need to be defined that establish strong baselines upon the commissioning of a BES Cyber Asset and tools need to be in place to notify and alert when variations to that baseline occur. Implementing Change Ticketing/Service Management solutions to provide the documentation of change records, GRC to aggregate that data and correlate it to a control, and security tools such as Tripwire and the Orion Gateways are all part of a holistic approach to a successful and efficient Configuration Management Program.

Suggested Solutions:

NovaTech®

The OrionLX Cyber Security Gateway accesses configurations from substation assets. These configurations are transferred to PAS Cyber Integrity for comparison to baseline.

tripwire

CONFIDENCE: SECURED

Tripwire's core functionality supports the process of formal change control and testing and offers exceptional change detection and investigation capabilities. Tripwire's Configuration Assessment Policy and Change audit features address the creation of a baseline configuration of computer systems and issues alerts and reports on changes. Following the process defined by NIST for POA&M reporting, Tripwire supports the tracking and authorization of changes to system baseline and configurations. Tripwire reports on security controls deployed, configured and their operational status. In addition, Tripwire baseline comparison operations can verify that a given test environment accurately reflects the production systems. This reporting supports this requirement.

The SigmaFlow solution provides compliant management of Approved Baselines. In the solution, Approved Baselines are created by OS type, Software, Hardware or any other common element that would apply to different Cyber Assets. Each Cyber Asset’s approved baseline is created by associating one or more Approved Baselines to the Cyber Asset. Through integration, the solution uses its Approved Baselines as a whitelist for Cyber Asset monitoring tools, and collects the “as is” settings of Cyber Assets for Validation within the SigmaFlow solution. The solution can automatically apply business rules to filter noisy data (ex. Port ranges can be applied to Ports with dynamically-assigned Ports) and reduce false positives. All issues are identified and alerted on, to ensure compliance to Baselines is maintained. Validation is typically run on a daily basis.

CHALLENGE 8: Data Preservation as Part of Recovery Plans

NERC CIP Version 3

Not required in NERC CIP Version 3

NERC CIP Version 5

A new requirement, CIP-009-5 R1.5 mandates the preservation of data related to triggering the initiation of a Recovery Plan. This preserved data can then be analyzed and diagnosed. The logic behind this requirement is that by referencing data that triggered past activation of a Recovery Plan, the probability of reoccurrence can be reduced.

Consequences:

With this additional component to Recovery Plans, the capability to analyze previous instances of an occurrence that would trigger a Recovery Plan is going to be a new challenge from a compliance perspective even though, from a security perspective, this practice has been in place across a variety of industries for some time. Data preservation controls and policies must be established or improved to reflect CIP-009-5 R1.5

Suggested Strategies:

Enhancing process controls around data retention specific to recovery plans combined with the proper storage capabilities and a GRC solution to track the process workflow from beginning to end are the key components to meeting compliance with CIP-009-5 R1.5

Suggested Solutions:

SIGMAFLOW®

The SigmaFlow solution can be used to collect common information about Recovery Plans, including the ability to use a Recovery Plan workflow procedure to manage the process of implementing a “recovery.” The collected information can be analyzed, reported on, and presented in dashboards to help Utilities identify ways to improve Recovery plans and follow effective practices. Where workflow procedures are used, the solution can present this information to the people performing the procedure to aid them in leveraging the experiences from past events.

CHALLENGE 9: Securely Handling BES Cyber System Information

NERC CIP Version 3

CIP-003-3 R4 is the current Information Protection requirement that specifies a program be documented to "identify, classify, and protect information associated with Critical Cyber Assets"

NERC CIP Version 5

Contains an entire Reliability Standard devoted to secure handling of information -- CIP-011-1 "Information Protection." It also introduces "BES Cyber System Information" which NERC defines as:

" Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber Systems"

Access Controls also must be in place for all BES Cyber System Information and the assessment of adherence to the Information Protection Program is now required every 15 calendar months.

Consequences:

Although complying with the new standard will require additional effort, the results may be an improvement over Version 3. For example, a multi-level classification scheme is no longer required. Instead, a simpler approach to the identification and protection of BES Cyber System Information is included in the new standard.

Suggested Strategies:

A revamping of an entity's Information Protection Program will be required to address the expanded components of CIP-011-1. Also, while manual assessments for adherence to an Information Protection Program may have been sustainable under Version 3 of NERC CIP, the enforcement of access controls around BES Cyber System Information under Version 5 should force the industry to look at GRC technologies to help sustain and automate the process controls.

Suggested Solutions:

SIGMAFLOW®

The SigmaFlow solution includes the ability to track and manage BES Cyber System information by physical location, logical location, or other metadata attribute. The solution also includes the fine-grained permissions roles and user activity tracking within the solution to address secure handling of data/documents retained by the solution.

CHALLENGE 10: Updates to Existing CIP Documentation

NERC CIP Version 3

Required documentation delineated.

NERC CIP Version 5

Additional documentation addressing new standards and requirements required.

Suggested Strategies:

Entities should revisit their document management capabilities to determine if their current approach is sustainable for CIP Version 5 compliance.

Consequences:

Even entities with compliant and well-maintained documentation under NERC CIP Version 3 will find it challenging to achieve familiarity with the required documentation for Version 5. An awareness of the transitional differences between Versions 3 and 5 is essential.

Suggested Solutions:

SIGMAFLOW®

The SigmaFlow Compliance Manager solution includes the ability to manage CIP documentation for multiple versions of the CIP standards, provides the views and data relationships needed to collect additional information for new versions (expanding metadata on existing items, organizing data under new relationships) to complete the transition process for data-driven reports. The solution also includes a robust document review schedule for managing the ongoing process of reviewing and updating policies

and procedures – the ability to create, assign, track and manage tasks associated with transition activities.

Contacts for Additional Information:

Chris Humphreys
Phone: 904-347-7657
Email:
chumphreys@theanfieldgroup.com
Website: www.theanfieldgroup.com

Katherine Brocklehurst
Phone: 808-346-5800
Email:
kbrocklehurst@tripwire.com
Website: www.tripwire.com

Kevin Johnson
Phone: 570-498-4409
Email:
Kevin.Johnson@novatechweb.com
Website: www.novatechweb.com

Terry Schurter
Phone: 972-826-4353
Email:
tschurter@sigmaflow.com
Website: www.sigmaflow.com