

The CIP Program: Are We on the Right Path or at a Precipice?¹

Stephen Flanagan²

Introduction:

I want to thank you for the opportunity to speak to you today. When I volunteered to assist with this workshop I was hoping for a quiet corner in which I might make a modest contribution to your time spent here. When I was told I'd be the keynote speaker I was a bit overwhelmed. I never had such an honor thrust upon me. But when I was told that "the other guy that we really wanted canceled" – I felt much better. But I still want to provide you some value for your money – so I have a few things to say and will hopefully leave time for a few questions at the end.

This is now the time for the disclaimer. With advanced years my gray hair is often mistakenly associated with wisdom and authority – but nonetheless *the views I express are my own opinions, and do not necessarily reflect the view of the Commission as a whole nor any of the Commissioners*

I want to begin by saying that I believe what is being done today by people such as yourselves is important and exciting work. It is work that has an impact today and which will, if done correctly, establish a solid foundation for a more secure future. I'm sure you find your work challenging, at times frustrating, but seldom dull. It's my intent to take this opportunity to try to raise your sights above the stacks of paper that you face today to gain a glimpse of where we may be headed. And in the process I want to show how what we are doing today is an important first step that must be taken – one which must not lead to frustration and disillusionment but to a commitment to go forward.

I also want to stress that I come here with the intent to engage in a dialog with you as to what we can collaboratively do to make this program a success. The roles which each of us play in this are different – but they should be complementary, not confrontational. I have come to share my perspective and my insights with you. I also came to learn from you, to gain from your perspectives and insights. This is the way the program was designed and it's the only way that it can succeed.

Before I get into my vision for the CIP program into the future, I think it best to tell you a bit about my past. Everyone comes to the table with baggage from past lives which effect their perceptions. I'm certainly no exception. Let's start with the obvious - I'm old. Most people in the cyber field are young and enthusiastic and, dare I say it, impatient. But I've been in the electric energy sector for over 3 decades and I can tell

¹ Provided as keynote presentation for the Southwest Power Pool Regional Entity (SPP RE) Critical Infrastructure Protection (CIP) Cyber Security Workshop at the Hilton DFW Lakes, Grapevine, TX 76051 on May 11, 2011; original source at <http://www.spp.org/publications/2011%20Spring%20CIP%20Workshop.pdf>

² Stephen Flanagan, is a supervisory economist serving as a Branch Chief in the Division of Audits, Office of Enforcement of the Federal Energy Regulatory Commission.

you that things have changed. Things that we used to dream about are now reality – but the reality is not always exactly what we thought the dream would be. We dreamed of independent power producers, exempt wholesale generators, open access and merchant transmission developers – of unleashing the power of competition to transform the stodgy utility sector into a vibrant new industry. But we got Enron. So as I look forward I also look back – I see so much potential but I see the need to move with a measured pace.

But enough of the history of the electric industry – back to me. I am a Presbyterian. That means that I see people as flawed. We'd like to hope for altruism but we better expect self-interest. That means that we need to be watchful for those whose interests might not be for the common good – be it the greed of Enron or the fanaticism that brought us 9/11. We need to guard against such real threats. We need to have accountability.

I'm also a recovering consultant. I have seen the energy world from many sides - natural gas, electric, petroleum products. In the electric power sector I've worked for IOUs, public power, industrial, IPP, alternative energy –over several regulatory regimes. I understand the competing interests, motivations and real limits that exist. I see that one size does not fit all.

I was raised a Massachusetts Yankee, but, by the grace of God , I'm now a Southerner. I've also lived in the Pacific NW and worked for utilities and electric power interests that serve loads in almost every State in the continental US. So I know a bit about regional differences both in terms of infrastructure as well as cultures. But I've also seen that as different as we may be we all share a great many common interests.

I've been a regulator but I've also been regulated. I worked for DOE before there was a DOE. On the other hand, I was the managing partner in a successful public utility consulting firm, so I know what it's like to run a business on a budget, and also what it's like to be regulated by both the Feds and the States – just as many of you are today. So I think I have a fairly balanced take on the pros and cons of regulation and the costs that regulation can have upon the bottom line.

Finally I'm a professional. I was trained in economics, spent years developing software and managing LANs, conducted engineering studies along-side some top notch EEs, and assisted in all phases of legal intervention before FERC, State Commissions and Courts of Law. Why I even paid for degrees in EE and Law and have diplomas that hung on the walls of my home to prove it (but they have my kid's name on them). Oh, and I spent years conducting auditing of utilities books as an intervenor, keeping watch over the rates charged for power, transmission, interconnections and such like . Oh and then there's my current gig as Branch Chief in the Commission's Division of Audits. My duties have included the oversight of the activities of the Division in the Section 215 audit programs and also allowed me to dabble in demand response programs and the evaluation of compliance with the Commission transmission incentive efforts. So I have developed a multi-disciplined perspective.

So there are my biases when it comes to today's speech:

- I embrace change but believe it needs to be managed.
- I hope for the best in people, but I keep an eye on my neighbor.
- I understand that there are legitimate competing interests that need to be balanced.
- I recognize and respect regional differences but see a great deal of commonality amid the patchwork.
- I'm leery of over-regulation but acknowledge some regulation is a necessary evil.
- I believe that in order to make effective policy decisions you need to integrate a lot of specialized knowledge.

Now that the baggage has been checked let's turn our attention to the topic at hand.

The Critical Infrastructure Protection (CIP) Program:

Risk Areas

I will address this topic from the perspective of a FERC auditor. At FERC we have been tasked by Congress with providing oversight of the CIP program in the electric power sector. And so, as an auditor, the first thing that I ask myself is "what are the risks?" At the Commission we have oversight over a lot of entities in a lot of areas. And despite what some people believe we have limited staff and even more limited budget – not everyone in DC works for the government and even fewer work for FERC. So when we are exercising our oversight responsibilities we must target those whom we choose and we must also choose what we audit. An assessment of risk is essential when we do this. So when I look at the CIP program what do I see as the systemic risks in the program.

Well the primary risks for every participant in the program, and hence the risks to the program itself, can be expressed as three questions:

- **Is the entity concerned about CIP?**
- **How has the entity demonstrated its concern in a tangible manner?**
- **Is the tangible expression of concern effective in addressing the technical concern?**

So, let's turn to each of these and try to understand how this FERC auditor would approach the issue.

Corporate Culture:

Now the first area – the level of concern of the entity – gets us into an interesting area. It's termed "the culture of compliance." This term was coined by and for attorneys. And in case you didn't know it the Commission is just full of those people. In fact they hold most of the high level positions in my Office and even most of the Commissioners themselves are lawyers. So I need to tread carefully (*oh, and BTW this may be the ideal*

time for me to reiterate that the views I express are my own opinions and do not necessarily reflect the view of the Commission as a whole nor any of the Commissioners). I have a problem with this term “compliance.” In fact I think it’s bad terminology for the CIP program and gets us into the entire wrong mindset from the get-go. And why do I think this? Well although the term “compliance” has a more or less precise legal definition, its use among the uninitiated does not have the same connotations. I fear that when many hear the term they look more to Webster than Black as the dictionary of choice. And in Webster one is likely to find the word defined as:

Compliance:

–noun

1. the act of conforming, acquiescing, or yielding.
2. a tendency to yield readily to others, especially in a weak and subservient way.

How does that grab you?

Well in the case of some Commission rules and regs encouraging such behavior may be viewed as a good thing. Some rules are laid out and you need to toe the line. You ***must*** put costs of category A into cubbyhole Z in accord with the USofA (which, for you non accountant types, is not a patriotic designation but denotes the Uniform System of Accounts). But when it comes to the new NERC reliability regime this type of thinking may be counter-productive. And, at this point, let me go further to say that from now on *I not only do not speak on behalf of the Commission and the Commissioners but perhaps not on behalf of my boss, the Director of Audits or even my fellow auditors at the Commission.* But, in my opinion, for reliability, and I stick CIP into the reliability program as a whole in this discussion, I think the better term would be “commitment” rather than “compliance.”

Why “commitment” you may ask. Well again Mr. Webster provides some helpful insights:

Commitment:

–noun

1. the act of committing, pledging, or engaging oneself.
2. a pledge or promise; obligation
3. engagement; involvement:

Now doesn’t that sound a whole lot better? I know that the words commitment and engagement scare some people today. But I believe only by being rooted in such concepts that this program can succeed.

In fact, as an auditor, I think that if an entity has a culture of “compliance” – and views it’s CIP program as yielding in a passive weak manner to some level of conformity to the standards – then I view that entity as a member of the high risk programs. On the other hand if an entity has a culture of “commitment” to its CIP program, one that embraces the standards as a part of achieving security, then I view the risks as far lower. I’ll try to get

more into exactly what it is that you should be committed *to* in a minute, but I'll ask you to hold that thought for a moment.

Now I don't want this to be a merely a matter of semantics. I'm sure that my lawyer friends would quickly tell me that I'm wrong in casting the term in this manner. But I think it has merit. Many entities view the reliability program (and particularly) the CIP program in just these terms. "That's the law – and, by the way, there's a BIG penalty if you don't do it. So we'll bend our backs and do what we're told – but not an inch more mind you!" [And between you and me, in many entities these people are usually called compliance officers – and they view their role as ensuring that the entity meets the literal letter of any standard but no more, under the pain of death – or something far worse.] But the relevant point here is that the standards are not "issued from on high" by the government but are industry-driven. They have been developed and approved by stakeholders in the electric industry. And not even the Commission can alter that fact (even if it really, really, really wanted to do so). But I don't want to go too deeply into this arena (*i.e.*, standards development) as I'm trying to wear my auditor's cap today. However, as I will opine at greater length and more detail later, a culture of commitment will impact the manner in which the CIP program is implemented in an entity and therefore the success of failure of the effort.

So, to sum up my take on this – when I consider the first risk in the CIP program I look to the level of commitment an entity has to the program. As an auditor some leading indicators in this area are:

1. Involvement of Senior Management
2. Level of Budgeting and How that Budget is Allocated
3. Staffing
4. Saturation Level

The first three of these are rather obvious – the last is a term I've coined for this occasion to connote the degree that awareness of reliability/security. And also how the awareness has permeated the manner in which an entity conducts its everyday business. If concerns in these areas arise in the same cyclical pattern as the compliance audit – then I would say there is not a high saturation level. But if the rank and file have a conscious awareness of, and concern for, these areas then the entity is highly saturated – its culture is great. Now developing a precise saturation level metric is still a work in progress. In an audit context it is usually clearly demonstrated in the interview process.

Tangible Demonstration of Concern

We can now move to the second area of risk: the manner in which an entity displays its concerns in a tangible manner. Now in the CIP space, during a compliance audit, the industry has provided to me the criteria by which concern must be demonstrated. In this area, I as an auditor have been given an industry-approved yardstick by which to measure (*i.e.*, quantify) an entity's concern for reliability. And the yardstick the industry has

given me is the current set of CIP standards. Am I thrilled by the measuring tool? Do I think that I might be able to contrive a better one? Would I like to “interpret” the yardstick as transformed in a dialectic manner from what it is to what it ought to be? All of these questions are interesting and perhaps even profound – but they are also equally irrelevant. As a FERC auditor I must play with the hand which I have been dealt. The CIP standards are what they are and so we must proceed along the path that they have delineated.

Which brings us to a series of often-asked questions. You might term these the FAQs of the CIP program. My personal list includes the following:

- Do the CIP standards really help reliability?
- Won't following the standards result in less, rather than more, reliability?
- Isn't this all merely a paper chase?
- Can identifying each blasted printer as a TFE ,because there isn't any anti-virus installed, really going to make my entity more secure?

I'm sure some of you have others – I'd open the floor for suggestions but then I'd probably have no time to finish my prepared statement – and that wouldn't work. This speech is after all about me – about my perspectives. So let me attempt to deal with a bit of this sort of sentiment.

Let me begin by giving you my perspective on what a reliability audit should be. I realize that this may not always happen. Every auditor has a bad day. Every party being audited may have one as well. Mistakes are made, things get overlooked, misplaced or misinterpreted. But on balance an audit should be able take the pulse of an entity. An audit is like a physical exam. You go to the doctor to get a physical. When I was a kid you went to one doctor for everything. He could, in one hour, check everything and give you a clean bill of health or get you patched up good as new in no time. But today we go to specialists – the human body has changed, now it requires one doctor half a day to check out one part. He takes dozens of tests which take weeks to process and when it's done he tells you that he didn't find anything wrong - but that's no guarantee there's nothing *really* wrong. That's what a NERC compliance audit is, a modern physical exam. You get an exam for Order 693 and then you get one for Order 706 and pretty soon there may be another for Order 999 – who knows?

So why do we perform audits? Or better yet, why do *you* agree to undergo them? Well it should be for the same reason that you go to the doctor. You want to have some level of confidence that things are going along OK. And when you go to the doctor most people are willing to take their clothes off in order to be examined. They open themselves up to the process. Why – because they really want to know that things are OK. And that's what should happen on a reliability audit. But is that your reaction? I doubt it. I bet you want to keep all your clothes on – you might even think that the layered look is back when the auditor comes through the door. Be honest isn't that how you really feel?

What can change this? Well I think it's a matter of trust. And maybe that comes from experience. Hey the last time you went to the doctor he did get a little heavy-handed about those extra 20 pounds. But now that you've lost them don't you really feel better. And even if that doesn't make up for the loss of satisfaction that those high cholesterol foods you gave up – you have achieved the goal of better health. And that's why you went to begin with.

At FERC we see conversions to this way of thinking more than you might expect. Let me give you a recent example. During one audit there was some difficulty in having all the information an SME provided in response to an audit data request cleared by the head of the division. The reviewer withheld some of the material, believing that it went beyond precisely what had been asked. However, the inclusion of the material would have been more helpful for the audit team to understand the issue they were examining. The management member who assisted us in getting the more complete response had the following to say:

I'll admit after almost 25 years of responding to *litigation* discovery requests, as a result of our discussions, I've had to more fully analyze my own approach to responding to *audit* data requests.

She had seen the light. An audit is there to make your program better. But it can't do that unless you allow it to happen. The layered look is out of fashion. Audits provide a window an opportunity to assess the manner in which the entity is actually able to perform in a manner to reach its goal. You need to open up the blinds and let the light shine in.

So with this in mind let's take a look at some of the current standards that may be giving rise to the FAQs and see if we might be able to develop a level of trust so that we can get through this together.

The CIP standards were put in place to address a concern regarding the vulnerabilities of the electric power grid to threats by parties seeking to deliberately adversely impact reliability. This is in marked contrast to the other reliability standards which were implemented with the premise that no party would seek to intentionally adversely impact reliability (although they may well seek to avoid paying their fair share to ensure reliability and hence lower the reliability as a byproduct). I think that at this point in time there are few people who do not believe that such threats are real and perhaps becoming more serious with the passage of time. I say this notwithstanding an awareness that there is some skepticism that the threats may be being exaggerated in the self interest of those who might benefit from expenditures made in greater levels of security. However, my comments will not go into this topic because I believe that this audience is keenly aware of real threats to the grid security and the fact that vulnerabilities exist.

I also believe that the current standards are certainly not adequate to address the concerns that we as an industry face. There is universal agreement on this, so it would be a bit of a red herring to throw that argument into the mix. There are many parties working long

hours on seeking to develop improvements to current standards and new standards to fill gaps in the existing standards. But again this is not where *this* talk is headed.

So having cleared the air on these points let's get our hands dirty with the current standards. I proceed with the assumption that the standards do relate to reliability and that in some manner they are intended to serve as an indication that entities are making efforts to maintain or enhance reliability. I base this assumption upon the fact that the entire reliability program rests upon the good faith efforts of the industry to keep the grid secure and reliable. If this foundation proves faulty then the entire edifice will fall. Therefore, despite their infirmities and blemishes the CIP standards must be viewed as a first attempt to develop what is needed.

The determination of commitment to current CIP standards is, under the NERC program, largely based upon a review of paper. In some instances the current manner in which compliance is being determined requires entities to generate and auditors to review lots of paper (either actual or virtual). At times it seems that what's on the paper is not so much important as the fact that the paper exists. Its being itself is its justification.

Unfortunately in some audits this has been the process and outcome. One is required to have a policy, procedure or process on a particular matter. But one is not told many (if any) specifics regarding how that should be structured. At times certain generic content is required but the vagueness with which true substance is required is amazing. Why is this the case? I would argue it rests upon the assumption that good faith efforts are being made by the registered entities and the fact that the various interests could not arrive at a consensus as to what the appropriate policy should be. And there's the precedent that standards should focus on the "what" rather than the "how." At least a portion of this problem is that it may be difficult to formulate a standard that can serve both as a yardstick to auditors that be equally applicable to all entities. What may be perceived as absolutely required of one entity may in fact be of little effective value to another entity. And finally, trying to focus on some minimal standard would hardly be likely to result in a secure, reliable grid given the threats. So at present we have standards that largely require a review of paper and which have limited specificity. Not the ideal situation by any means.

But faced with such a situation should the auditor resort to a check the box paper review. Is that all there is? I think not.

Let's get back to the concept of a good faith effort being made. Or as Gerry Cauley, the current head of NERC is wont to say, "trust but verify." Does the verification stop with seeing a piece of paper – or in this instance a whole lot of paper? No, it should not. Good faith efforts should embrace not only that the paper exists, but that the paper demonstrates that efforts to address the underlying technical concerns are underway and that the manner in which these concerns are addressed has technical rigor. In other words that it's neither a sham nor a weak and subservient response to do as little as possible.

The audit team should therefore be looking into the substance of the policies, procedures and processes (the 3 Ps). The audit team should examine how these enable the entity to

meaningfully address the technical concerns at hand. When the audit team believes that the 3 Ps lack the technical rigor necessary to address the underlying technical concerns, they should make a finding to that effect.

To summarize, in order for there to be a tangible demonstration of concern in the compliance audits by the entities, they must show, and the auditors must evaluate, that:

- There are existing policies, procedures and processes
- That these address the underlying technical objective of the standard
- The manner in which the objective is addressed has technical rigor

I believe there is a good degree of latitude in professional judgment that can and should be employed to determine the appropriate technical rigor required. But the fact that such discretion needs to be exercised should not become an excuse for not rendering any professional judgment. Concerns in these areas need to be addressed and conveyed to both NERC and FERC to allow them to fulfill their roles in the program by facilitating the development of appropriate standards and providing oversight of the program.

Performance: How Effective has the Entity Implemented Its Program

Up until this point in my discussion I have stayed with the concept that the audit of the CIP program of an entity should proceed along the line of a documentation review. I did this because, in the main, the current approach NERC adopted to determine compliance focused primarily, if not exclusively, upon compliance to existing standards measured in terms of the documents. But now I am going to go the final step – the step that I feel a FERC auditor should in fact take in this area. And this final step is to assess performance in implementing the CIP program.

The best sounding policies, procedures and processes are worthless in achieving the goal of the program (i.e. grid security in the case of CIP) until and unless they are effectively implemented. Therefore, the auditor must examine the implementation in order to assess the effectiveness, efficiency and economy in achieving the technical objective. This area is one that a lot of people are thinking long and hard about. Of particular concern is the development of performance-based standards within the compliance regime. Better minds than mine are at work on this issue, and it is essential that we get it right. Ultimately, we need performance-based standards that will incentivize the industry to adopt (and perhaps develop) the best practices applicable to a specific entity.

This is not just my opinion. I believe it was the opinion expressed by the Commission in its Guidance Order regarding the NERC compliance audit program issued in January 2009. In that Order the Commission urged audit teams to examine, discuss and report areas of concern which were not current violations but which may rise to the level of a violation in the future. Some have asked how an auditor might know about such a situation. Does one need to be prescient – to foresee where a future standards will be in order to anticipate a violation? I don't believe so. I understand that this guidance was

based on an understanding that, under the assumption of a good faith effort by the industry, gaps would eventually be filled in current standards that are necessary to ensure technical objectives. Therefore, current failures in the performance to achieve these objectives, not addressed in current standards, would need to be addressed in future standards. And unless these performance issues were addressed by the entity prior to the emergence of the new standards, there would be future compliance violations.

In addition to the Commission guidance, there is another key indicator that collaborates my perspective. In a recently released audit report by the Department of Energy Inspector General of FERC the need for performance-based auditing to address issues not covered by the current standards was a key element. I'll not go into this report at any depth at this time, but the report recognized that examining the ability of the current participants' ability to meet the program objectives needed to go beyond review of compliance to the existing standards. FERC is of course seeking to address the recommendations in this audit report (and my being here today is part of that commitment) and I believe that NERC and the industry need to think carefully about them as well.

For the CIP standards a performance-based approach would require the auditor to interview the single senior manager with overall responsibility and authority for **leading and managing** the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3 [CIP003]. This interview would elicit the technical objective of the CIP program and how current policies, practices and procedures are meant to achieve this objective at an appropriate level. This information would provide an internally generated yardstick upon which to evaluate the effectiveness of many key performance areas within the entity's program. The interview may also heighten awareness to possible gaps in the program. This approach would allow performance to be measured in terms specific to the program needed for a particular entity to achieve its desired level of security.

As an economist, I like this approach because it incorporates two important elements; appropriateness and sustainability. As I said earlier the concept to appropriateness must be considered in the CIP program. One size does not fit all – but there should be a size found that appropriately fits the entity being audited. The ability of the entity to recognize the objective and develop a program that will accomplish this objective within the entity is the key concept. Sustainability flows out of this effort to find an appropriate application. Sustainability indicates both that the efforts issue forth from the manner in which the entity operates – it's as natural as breathing – and also that it does not require external forces to keep it going. Programs that exist only due to outside pressure (e.g. the audit) are really not sustainable. If left to itself, entropy will gradually bring such a program to a halt.

The audit would test two elements, rigor and robustness, thereby addressing the manner in which the procedures adequately address the stated objectives in compliance with the NERC standards. Note that this is not an either/or but a both/and approach. Where current procedures violate the standards, a compliance violation would be indicated. And whenever inadequacies in the procedures are revealed that hinder the ability to achieve

the objectives, these would be noted. I would expect that often there would be an overlap of the two findings. Such an overlap would indicate that the current standards specify elements necessary to achieve program objectives. However, areas in which current standards/requirements are not violated, and yet performance is lacking may indicate the need for additional or improved standards/requirements but no violations would occur.

A measure of the success in the meshing of the performance of an entity's CIP program and the current compliance documentation requirements can be seen when the documents required for compliance are an integral part of how an entity carries out its routine operations. When these reporting requirements flow naturally from the process, rather than being a separate "done for compliance audit" process. As an auditor, when I'm given documentation in support of compliance, I seek to determine the provenance of the document. If I discover that its *raison d'être* is the audit, I'm a bit skeptical that it reflects the actual operations of the entity. Red lights start blinking and warning sirens sound. Documents that support compliance should flow out of the normal work processes of an entity. If they don't, then something is wrong – either with the standard, its applicability to the entity, or the entity's program.

When conducting such a performance review the auditor needs to exercise his professional judgment to urge the entity to deal with failures in performance. However, he must be sensitive to the constraints upon the ability of the entity to achieve higher levels of performance and attempt to conduct a type of triage in his audit recommendations. At points at which the performance audit has disclosed clear inadequacies that pose a danger, he should recommend they be mitigated with due dispatch. In areas in which improvements need to be made, but no immediate threat to reliability is perceived, he should address the need for improvements to be made to avoid future violations. Finally, in areas in which the auditors can promote best practices to achieve greater effectiveness and efficiency in the program, they should make such suggestions for the consideration of the entity. Finally, the audit team needs to include all three categories of concern in its audit report.

The goal of the performance audit is to assess the entity's ability to meet the program goal – security. It is targeted to identifying areas of the current program which will prevent or inhibit achievement of the objectives. It goes beyond current standards – beyond compliance to existing standards. It serves to identify current standard inadequacies, pave the way for higher levels of performance and move the industry to the actual achievement of security goals. Therefore, its primary purpose is to strengthen security of the grid not issue violations.

It's at this point that I will close this section by discussing an incident that happened in a real world CIP audit. I think it shows the tension that exists within the CIP compliance world - one that needs to be avoided.

In the early CIP Spot Checks an SME at one large entity explained to the audit team that he and an assistant routinely manually produced tables showing that all persons who had access the critical cyber assets had been properly vetted. In order to accomplish this task

a tremendous effort was required, since the relevant information resided on four separate databases, scattered across the enterprise, and not link to each other. He estimated that it took about 20 days to process this information manually and it was done quarterly. This procedure had been implemented in response to the new CIP standard. All of the paperwork was in binders that the members of the audit team were free to wade through and sample to their hearts' content.

But let's ask ourselves whether this made the bulk electric system more reliable, more secure. Clearly, producing the reports did not directly accomplish these goals. In fact, one might argue that taking a security officer and his assistant off the watch to put this all together actually might have made things less reliable. But is this really the way to look at the issue? I think not. The issue was why the entity focused on the perceived need for a specially created report – one that needed to be created manually every quarter in order to be included in the papers for an audit. Why was this being done in this manner? Was the focus the entity's commitment to ensuring that the specific staff with access to the critical assets were being trained and made aware? It did not appear to be the case.

My take in this instance was that performance was lacking. What was needed was an effective and efficient control to ensure that training and awareness information was being provided to the appropriate persons (i.e. the CIP04 standard). A manual report done quarterly was not what was needed to achieve the objective of the standard – it was what was perceived to be needed to meet the measure of the standard (i.e. to achieve compliance). Rather than address the performance issue, the entity focused on the compliance issue. This resulted in generating paper in lieu of enhancing performance that might strengthen security. The entity could have achieved both, but opted for the short term “quick fix.” Had the audit addressed performance the entity's behavior would have been brought into proper alignment with the objectives of the program. The proof of this was demonstrated when the audit team had asked that a report of the current status of just seven employees be produced for review during the on-site audit. Given the disjointed data collection efforts involved, the SME was unable to assemble the data within 48 hours. Instead, in lieu of the specific data requested, the pre-prepared reports for the prior period were provided and deemed compliant.

I think that's an important “lesson learned” from my audit experience. Perhaps in my time here with you, we can share such lessons with each other and get closer to making this program become what it needs to be.

The key points to the performance-based auditing that I am advocating is:

- Performance to Meet the Specific Entity Goals Must be Assessed
- Correction to Performance Should Follow Risk-Based Criteria
- Security Not Violations is the Primary Focus

I believe that these program elements can and should be incorporated within the current auditing context. Inclusion of these points will go directly to addressing the CIP program

objectives and move the industry to rapidly address the threats and vulnerabilities that face the industry. There have been other proposals and initiatives suggested in this critical area. The recent NERC effort to conduct Sufficiency Reviews for the identification of critical assets and the use of peer-review audits within the industry are two such examples. However, these efforts, while helpful, do not allow FERC the ability to gain the insights into the status of the grid security which is necessary to carry out its oversight responsibilities.

Conclusion

Let me conclude by summarizing the three risks that the CIP program faces and what needs to be done. And in so doing I will amend my initial points to reflect the emphasis on the performance to achieve the goals perspective.

- **Is the entity concerned about CIP?**
 - Senior Management Needs to be Committed/Engaged/Involved
 - Sufficient Budgeting Must be Available To Achieve the Goal-Oriented Tasks
 - Staffing Must be Directed Towards Achieving Program Goals, Not Disconnected Compliance Activities
 - The Saturation Level of Security Awareness Must be High

- **How has the entity demonstrated its concern in a tangible manner?**
 - Existing Policies, Procedures and Processes (3 Ps) Must be Designed to Meet the Program Objectives and be Clearly Understood by All
 - These 3 Ps Address the Underlying Technical Objective not limited to the Language of the Standards
 - The Manner in which the Objective is Addressed Must Have Technical Rigor

- **Is the tangible expression of concern effective in addressing the technical concern?**
 - Performance to Meet the Specific Entity Goals Must Be Assessed
 - Correction to Performance Should Follow Risk-Based Criteria
 - Security Not Violations is the Primary Focus

As I stated at the beginning these are times of great challenge and great opportunity. Not only the present but the future is at stake. You assembled in this room have great talents and abilities – far greater than my own. Please – commitment yourselves to the task and move this program forward.

And with that I will conclude my speech – which I will term my “opening affirmative statement”, as my children do in their debate rounds, by saying – “I urge a vote for the affirmative position and stand ready for cross examination.” Thank you.