Webinar: Get Ready for Version 4!

March 27, 2013 / 8:30am – 9:30am PT

Archive: http://grids.ec/getready4version4

Host

Sponsor

Honeywell

Questions and Answers

These questions were taken from the live webinar. The presenters have taken time to respond to each of them in kind. The questions are in no particular order.

Q: **Can you define a 'Routable Protocol'?**

A: There are only two NERC resources describing this term:

(1) CIP version 1 Frequently Asked Questions (FAQ), CIP-002-1 question #6m, page 5: http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf;

(2) Guideline for Identification of CCAs, page 25, http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf.

The term is not in the NERC Glossary of Terms, nor is it included in the CIP version 5 draft standards. Generally for NERC CIP, the most common routable protocol [and the only one we have encountered to date] is IP (Internet Protocol) because it contains both a device address and a network address that allows it to be forwarded from one network to another.

Decnet is sometimes used in control center environments and could be considered routable depending on the context. Also, auditors will look at MPLS as a possible routable protocol.

Disclaimer: The answers to these questions are based on the webinar panelists collective knowledge as they currently understand NERC CIP applicability and general audit approaches.. The panelists **encourage all utilities to engage** NERC and the Regional Entity CIP auditors to obtain authoritative answers. There is no guarantee that these responses are 100% accurate; however, it is reasonable to assume that they qualified responses.

Q: **"Push back by a year" meaning April 1, 2015? for V4?**

A: This is what was suggested in Tom Alrich's this blog post (actually he said six to twelve months. Even six would be a big help). However, this would require two things:

1) NERC would have to petition FERC to do so, and

2) FERC would have to grant it.

Unfortunately there isn't a lot of inclination to do either of those, so this is a very long shot.

Q: **What's new or different in v4 from v3? You didn't touch on any of that today.**

A: The only difference between V4 and V3 is CIP-002; primarily the fact that the entity doesn't develop a risk-based assessment methodology (RBAM) to identify Critical Assets. The RBAM is a Responsible Entity defined methodology. Due to a perception that this approach did not result in a sufficient number of assets being declared as Critical, the approach was changed in CIP-002-4. Now, everyone shall follow the industry-defined bright-line criteria. There are also some changes in how Critical Cyber Assets are identified (again, all in CIP-002-4).

Q: **Should we get rid of our dial-up technologies for CIPv4?**

A: The handling of dial-up in CIP versions 1-3, does not change in version 4. It is not so much a question about the CIP version, but the challenges you will face trying to comply with CIP-005 access control and logging requirements for dial-up connections. If you do not have a dial-up access solution that is compliant with CIP-005, then you should consider the cost of that upgrade versus re-architecting to use a serial and/or routable protocol-based solution.

Q: **Are customer generators that feed into grid (solar for example) included in CIPv4?**

A: There is a sequence of events/activities that must occur before generation is included in CIPv4. First, do you have sufficient generating capacity to meet the threshold (i.e., single unit >20MVA, multiple units >75MVA) of:

- Appendix 5B (http://www.nerc.com/files/Appendix_5B_RegistrationCriteria_20120131.pdf)

- of the NERC Rules of Procedure (http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20100610.pdf) ;

- Appendix 5A (http://www.nerc.com/files/Appendix_5A_OrganizationRegistration_20120131.pdf) provides information on the registration process.

After NERC registration, then all entities must comply with CIP-002-4 and determine if there are generating stations that meet or exceed the bright-line criteria in Attachment 1. All Registered Entities must go through this exercise of determining if they have Critical Asset facilities or not, and storing such evidence of results annually.

Q: **Are radial 115kv Substations included in CIPv4?**

A: No, they wouldn't meet the bright-line criteria for two reasons. One is that only transmission substations are included. The second is that only substations operated at 300kV or higher are included.

Q: **Our control center will not be a critical asset per the version 4 brightline. Should we revise our version 3 RBAM to use the same risk criteria as Version 4 uses?**

A: Most of the Regional Entities had said that this was not permitted. However, this is changing rapidly. You should check with your Regional Entity. However, you will most likely have to use the entire set of bright line criteria in Version 4; you won't be allowed to pick and choose from them.

Q: **The timeline in Phase 4+ is longer than the due date, are you saying that phase 4 needs to be completed before the 4/1 due date?**

A: The timeline for Phase 4+ provided information on the actual time that companies have needed to achieve compliance; it is not the time available. The timeline slide is intended to illustrate the magnitude of work required, and only 1 year to complete it. The fact is that – for every facility that meets the bright-line criteria in CIP-002-4 Attachment 1 – full compliance with every requirement in Version 4 is due on 4/1/2014. The only exceptions for this are assets that

were not commissioned before June 25, 2012, the date that Order 761 was published in the Federal Register

Q: **While cryptographic keys and certificates are addressed specifically in CIP v5, functionally they are essentially password files, passwords being included in CIP v4. In the spirit of due diligence, should evaluating keys and certificates be included in access control audits for Cyber Assets?**

A: Throughout the NERC Standards, anytime there is ambiguity or lack of direction related to any situation, scenario, or technology – we recommend that you document the interpretation that your entity intends to follow. This ensures there is consistency in its application, and the Auditor can follow your process to have the same result. Additionally, you can submit your interpretation to NERC as a Request for Interpretation (RFI) that is reviewed and voted upon by the NERC membership. Many of the appendices to the CIP Standards are a result of RFIs. There are no resources from NERC (that we can find) that contrast cryptographic keys and certificates as password files. Technically, I agree; but that is our independent and individual interpretation – which may or may not be supported by the NERC membership. There are no requirements in the CIP Standards, there are no RFIs, therefore there is no need to evaluate keys or certificates to achieve compliance. If performed, which is a good security practice, it would be for cyber security reasons only – not for CIP compliance.

Q: **If you have multiple Cyber Assets in a common panel do you have to evaluate that as one item or can you still evaluate each of the items internal to that cabinet? Basically if you can ignore the cabinet everything internal is redundant so no one item would cause generation issues within 15 minutes.**

A: We consider the panel as a metal box, or physical perimeter, containing the individual Cyber Assets. Each component would be evaluated individually; you are not permitted to summarize the Cyber Asset as a box with "other stuff inside". Secondly, redundancy is not permitted as sole criterion for 15 minutes impact because we must also consider degradation or compromise (e.g., malicious use, tampering). Security vulnerabilities and cyber attacks are non-discriminatory and will impact both the primary and redundant devices equally. See the NERC Guideline for Identification of CCAs for more info:

http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf.

Q: **On a power plant if you locate your controllers for the DCS in the control room and not in the remote I/O cabinets would that remote I/O cabinet be considered critical?**

A: Following our process, we must first go through a number of logical steps before we can make the determination that the remote I/O cabinets are Critical Cyber Assets. First, do the remote I/O cabinets fulfill a function that is essential to the operation of the DCS; I assume they do and it has zero relevance on the location of the remote I/O cabinets. At this point, we consider the remote I/O cabinets to be "essential cyber assets" and the next step is to evaluate their connectivity. If they use non-routable communications (e.g., DH+, LCN, serial) from the DCS controllers to the remote cabinets, then they would not be qualified as Critical Cyber Assets. If they use routable communications (e.g., ModBus/TCP, IP) from the DCS controllers to the remote cabinets, then both the DCS controllers and the remote cabinets are qualified as Critical Cyber Assets and subject to CIP-003 thru CIP-009. In summary, it is not possible to make a determination of what is critical without first understanding what is performing an essential function, followed by an evaluation of its connectivity.

Q: **When the preliminary cyber asset list is being created in a generation facility, wouldn't it be better to start evaluating the devices based on the "shared" and "15 minute" criteria before looking at the essential functions to quickly eliminate devices that do not meet the shared and 15-minute criteria?**

Q: **It is feasible to slim down the CIP-002 process by performing a functional review starting with the reliability functions and coming up with cyber assets that are associated with those functions. At plants especially, there are so many devices like controllers that are equipment based rather than associated with a reliability function that the owner may be spending time and money identifying and cataloging equipment that is not CIP related.**

A: Focusing on the "shared" and "15 minute" criteria will be the fastest approach. The first concern is ensuring nothing is missed, which is ultimately a function of your confidence in the understanding of the generating facility, its functions, its systems, its cyber assets, and how they are inter-dependent. The second concern is ensuring the CIP-002-4 compliance record is sufficiently detailed and accurate that it would satisfy a compliance audit with timely responses to information requests; for every Cyber Asset in the facility. We don't recommend shortcuts on CIP-002-4, as it lays the foundation and scope for compliance with CIP-003 thru CIP-009. We recommend over-preparing, over-collecting, and indisputably determining which are your Critical Cyber Assets in a manner that can be easily verified in the future.

Q: **Please address how granular the CCA list must be: i.e. to the critical function, to the box, to the circuit board, etc.**

A: For compliance, the CCA list must contain enough information to correlate the logical cyber asset list to the physical device(s) (e.g., hostname, serial number, location, IP address, other unique identifier) in the facility. It is recommended that in your documentation a line can be drawn from the essential functions, to the supporting Cyber Assets, and the physical device that fulfills it. For example, if the Exciter is essential to the generator, what are all the Cyber Assets that support its operation = why is the Cyber Asset on the list in the first place? As for granularity, a preliminary line is drawn around those components that support serial connectivity (a source for dial-up), Ethernet interfaces (a source for routable connectivity), wireless (a source for routable connectivity) when complying with CIP versions 1-4. As for a circuit board, this has a lot of meanings depending on the type of device in question. If it is a standard PC, then the motherboard and all the PCI/PCIe/AGP cards are part of the same Cyber Asset. If it is a controller backplane with multiple cards inserted into it for various functionality, that can all be interpreted as the same Cyber Asset. In many Cyber Asset lists, the unique identifiers are the device hostname and its IP address.

If you are using virtualization, know that if any one of the virtual machines is considered critical, then so is the host server hardware. As for distinction on the Cyber Asset list: the host is one Cyber Asset; each virtual machine is its own entry on the Cyber Asset list.

Q: **Do FERC's March 21, 2013 Orders remanding 2 of NERC's interpretations on "wires" and "essential cyber assets" affect the way entities should approach these two issues in version 4?**

A: Unfortunately yes, since CIP-003 through CIP-009 haven't changed at all between V3 and V4. Of course, it would be a big discussion to say what exactly you need to do differently because of those two FERC Orders. We can say that you need to start treating laptops or remote PC's that are used to operate BES control systems as Critical Cyber Assets. The remand of the interpretation on essential cyber assets could also affect how CAN-005 is viewed and handled by audit teams.

Q: **Why wouldn't you ask NERC or FERC staff and at least get a preliminary interpretation on the asset that is 50-50 owned?**

Q: **Please address handling of jointly owned facilities/assets that are considered Critical by one party and non-critical by another.**

A: Because NERC and FERC staff won't do that. It's up to the two owners to decide who is responsible for compliance. There is additional information in the NERC Rules of Procedure Section 507 and Section III Organization Registration Process. Also, see this passage in the CIP V4 Rationale and Interpretation document:

> *A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.*

Q: **Please clarify your comments on the "quarterly review" of access lists. Is this effort to verify that all paperwork was processed and retained correctly, a double-check of changes for accuracy (i.e., administrative review). . . or are we only talking about the ""managers"" of the employees on the list reviewing that those individuals are, indeed, the ones who still need access?**

A: Many entities fulfill the quarterly review of access lists by having the owner of the resource (e.g., a Cyber Asset, an application) review the list of who currently has access, and validating they still need access. The paperwork processing and retention is equally important, because you cannot prove you performed the quarterly review without the evidence.

Q: **What external resources do you recommend for planning and vetting V-4 and V-5 RBAM**

A: There is no RBAM in V4 or V5, just bright-line criteria (and the BLC are different between the two versions). However, we think your point is that you should have expert assistance in applying those criteria, since they are subject to a lot of interpretation. We completely agree with that, and if you want to email Tom Alrich at tom.alrich@honeywell.com he can recommend a list of several qualified firms that can do that (Full disclosure: Honeywell provides services for everything else in CIP V4 except for BLC application).

Tom Alrich has suggested in this post that NERC should develop a guidance document to help entities interpret the BLC. There is also the Version 4 Rationale and Implementation Reference Document, which was approved with the standards and therefore has some official standing.

Q: **Please provide more info on Data Diodes**

Disclaimer: The answers to these questions are based on the webinar panelists collective knowledge as they currently understand NERC CIP applicability and general audit approaches.. The panelists **encourage all utilities to engage** NERC and the Regional Entity CIP auditors to obtain authoritative answers. There is no guarantee that these responses are 100% accurate; however, it is reasonable to assume that they qualified responses.

A: Data diodes are an electronic device that only permits one-way communications. They can ensure traffic from the high-trust zone (e.g., control system) goes to the low-trust zone (e.g., business network), but never can the low-trust zone send traffic to the high-trust zone. This is a concept originally used in military applications to ensure untrusted data cannot go into a high trust zone. In actual practice, they are a respectable security control for a network. Unfortunately, security and compliance are not always the same. Compliance Action Notice 24 (CAN-0024) was issued to help auditors evaluate the use of data diodes in non-control center situations; effectively stating that most data diodes are considered access points to the ESP, unless one is "embedded" and does not have an IP address. NERC has recently withdrawn CAN-0024 and the interpretation of data diodes remains in question again. At this time, data diodes are a respectable security solution, but I do not recommend them as a means to avoid CIP compliance.

A: The auditors will make their own determination on data diodes in each case in which they encounter them. Without CAN-0024 (to kick around), no entity can be sure what an individual auditor's judgment will be in a particular situation. If you simply put in a data diode and don't do anything else to comply with CIP in a facility, you are running the risk of very substantial fines if an auditor later determines there is still a routable protocol in use.

Q: **Explain how CIP-002-4 1.1 relates to different scenarios including same and different ownership, common ringbus, etc.**

A: Tom Alrich has stated in this post that the bright lines are not so bright, and need a lot of interpretation – your question simply affirms that fact. Tom has recommended that NERC develop a guidelines document for application of the BLC, as they did for Critical Asset identification in Versions 1-3. We recommend involving your Regional Entity for more specific scenarios. As mentioned above, the Version 4 Rationale and Implementation Reference Document can provide some help.

Q: **Do you have any guidance for entities that will be "de-listing" CCAs that no longer qualify with version 4?**

A: When preparing your compliance evidence, it should be version specific (i.e., version 3, version 4) for the period you are required to comply. The prior CIP-002-3 evidence is still valid and must be retained, while the CIP-002-4 does not have to come to the same result as the Critical Asset identification methodology has changed. If you are de-listing CCAs with version 4, there are others who envy you. However, pay close attention to CIP-002 version 5 and if that facility will have High or Medium Impact BES Cyber Assets. We have worked with

companies that have achieved compliance in 2009, but for whatever reason they failed to sustain compliance for some time and found it was equally difficult to get back into compliance, as it was to achieve compliance the first time. Some information associated with CIP compliance is atomic, in that it is only valid until the next change is made and it gets updated. The best examples are many of the CIP-007 requirements on patching, ports, services, and users that, if ignored for several years, require a complete refresh and redo to get back into compliance. The other challenge is re-institutionalizing the culture of security and compliance into each person again.

Q: **Have you considered the change in the definition of the Bulk Electric System and V4 inclusion of cranking path?**

A: At this time, we are not prepared to provide a qualified response. It is certain that the changes in the BES definition will have an impact on how assets are categorized; however, it is a bit early to realize those impacts.

Q: **Along the line of the grouping of ESP and CCAs, if there are multiple ESPs within one PSP, are the connections between the ESPs brought into the program?**

A: If you are stating there are multiple ESPs, also known as "discrete" ESPs, then I would suspect each has its own discrete access points. For example, network 192.168.0.0 is one ESP, network 172.16.1.0 is the other ESP, and 10.1.1.0 is the zone between them. As long as both 192.168.0.0 and 172.16.1.0 have their own access points, then the 10.1.1.0 network between them is exempted as per CIP-002-4 Applicability 4.2.2 "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters."

A: Be careful to ensure that the endpoints of the links between discrete ESPs are listed as access points and adhere to all relevant requirements. A common mistake is to think that traffic can be allowed to flow unrestricted between ESPs. This is not the case. Traffic leaving one ESP and entering another ESP must be treated at the access point the same as traffic from other untrusted networks.

Q: **I thought there was an 18-month implementation plan under v4 for newly identified assets?**

A: You have a lot of company; many others thought the same thing – but it's wrong. Tom Alrich has a blog post about this; please read that. Briefly, you have a 12-24 month implementation period under V4 for assets that are newly commissioned

or newly identified *after* 4/1/2014. But for assets that were in operation as of June 25 of 2012 (the day that FERC Order 761 was published in the Federal Registry), full compliance with CIP-002-4 through CIP-009-4 is due on 4/1/2014.

Q: **Assessment experience in nuclear power plants has found that many cyber assets can be logically grouped into a fairly small footprint of "cyber asset families". Are you finding this is a leveragable approach for NERC CIP v4 (and later for v5)?**

A: Grouping the cyber assets is performed inherently when trying to associate Cyber Assets to essential functions – as a group of devices are needed to fulfill the function. When looking at CIP v4, having the cyber assets grouped together helps to determine which need to be in a network zone (i.e., Electronic Security Perimeter) together, and those that can be moved outside the ESP. In CIP v5, the definition of BES Cyber System follows this thought more closely. From a security perspective and applying the ISA-99 Zone and Conduit concepts, putting groups of Cyber Assets into their own zones and protecting them will result in the best cyber security.

Q: **Since CAN-0024 was revoked on 3/1/2013, what are your thoughts about data diodes re: routable protocol connectivity?**

A: Before and after CAN-0024, we have not recommended the implementation of data diodes as a means of avoiding CIP compliance. They are respectable security perimeter devices, but we cannot confidently state or recommend they can be consistently interpreted as non-routable access points during the audit process. CAN-0024 allowed those data diodes which were embedded and did not have IP addresses to be considered non-routable access points, but it is too risky at this time to assume CAN-0024, or a future version, or CIP v5 will allow exemption from NERC CIP by their implementation.

Q: **When evaluating transmission equipment, would it be a good idea to include Microwave communications systems associated with relay protection?**

A: Yes, it is a good idea to include microwave communications systems equipment as part of the communication medium and links for your ESP. Microwave and other radio should be considered as communication links, similar to a fiber link between buildings. In this case, it becomes necessary to consider CIP-006 and its Appendix 1 related to non-physical measures to protect these links. Please note that, if these links are considered to be in the ESP, then the equipment supporting them comes into scope for CIP standards, and that can be difficult in

some situations. It might be better in some contexts to have discrete ESPs if the microwave gear cannot be protected.

Q: **Will there be any changes in fines for noncompliance?**

A: We cannot speculate, other than to refer to the list of fines to date and make inferences on the increasing values over time. There has been no change to the rules or processes for determining fines as a result of version 4. If the VRF or VSL for a requirement has changed, then it is possible fines will change as well.