CIP-004-5 HIGHLIGHTS

What’s New, What’s Not, What’s Hot!!
APPLICIBILITY

Registered Functions:
BA, DP, GO, GOP, IA, RC, TO, TOP

Applicable systems are classified according to how they fall into the CIP-002-5.1 identification and categorization process.
R1-Awareness Training

Table 1- Security Awareness Program

Really no change from the previous versions. Calls for the program to be presented once per Quarter in the form of:

- Direct communications such as E-Mail, memos
- Indirect communications such as posters, brochures
- Management Support-meetings or presentations

3/24/2015
R2-Training

Table 2- Training Programs
One or more programs applicable to individual roles and responsibilities.
Table 2.1-Basically the same as previous versions although it is a bit more specific regarding training directed for specific roles.

Does this mean I need to develop ten individual programs???
NO!!

You may choose to do so, but if you address all roles and responsibilities in one program that is acceptable.

Whichever method you choose you should be prepared to furnish the programs in whatever form they may be (power point, computer based, etc.) as evidence at audit.
R2 continued

Table 2.2-Training prior to granting access

This CERTAINLY sounds familiar, no changes here.

Training records will be requested to document that training was given prior to an individual being granted authorized unescorted access.
Table 2.3-Training cycle

OH, OH!! Something new!!

Training must be conducted once per 15 calendar months. This is specific to the standard and appears to answer the age old question ‘What is annual?’

Again, training records can be used to document compliance.
R3-PRAs

Table 3.1-Process to confirm identity:
No one process is called for in the standard, some common ones are: E-Verify, I-9 Forms, SSN Trace by a background screening company.

Nothing really different here.
Table 3.2- 7 Year Criminal Background check

Calls for:

3.2.1-Current residence
3.2.2-Residences in the past seven years

If you cannot get a seven year history due to a person coming from a foreign country or other factor, do as much as possible with documentation as to why the full seven years could not be completed. In some instances of foreign born individuals you may ask them to provide a “good conduct” letter from their country, which they can often obtain from their Country’s local Consulate or Mission.
R3 Continued

Table 3.3-Evaluate the criminal record and document the criteria used by your entity.

Table 3.4-Verification of PRAs for contractors or vendors. Document how you verify that PRAs were actually completed.

Table 3.5-Process to ensure PRAs every 7 years

Again, not really anything new in R3 except for the format.
R4-Authorization

Table 4.1-Process to authorize based on need:
Includes Electronic access, unescorted Physical access and access to BES storage areas

Table 4.2-Quarterly review of access privileges

This is not new.
R4-Continued

Table 4.3-Annual review of Electronic Access privileges –
Again defined in the standard as once every 15 months

Table 4.4-Annual Review for access to BES storage locations according to roles and responsibilities.

This is new.
R5-Revocation of Access

Table 5.1-Revoke unescorted and Interactive Remote Access \textbf{within 24 hours} upon \textbf{TERMINATION}.

Access MUST be revoked within 24 hours, if you choose to terminate someone on a Friday, plan to work on Saturday if necessary.

This is for a \textbf{TERMINATION} only!!
R5 Continued

Table 5.2-Reassignment or Transfer
Access must be revoked by the end of the next calendar day after the determination is made that the individual no longer needs access.

Table 5.3-Termination (can you say redundant?)
If you haven’t done so already as per Table 5.1, you must remove access to BES storage locations (both Physical and Electronic) by the end of the next calendar day.
R5 Continued

Table 5.4-Termination-again!!
You must remove access to non-shared user accounts within 30 calendar days.

Table 5.5-Termination-You must change passwords for shared accounts within 30 days.
For re-assignment or transfer-change passwords within 30 days after determination is made that the person no longer needs access or if extenuating circumstances exist, within 10 calendar days after the extenuating circumstances end.

Some new information in R5 but most entities were already pretty vigilant when it comes to revoking access.
Conclusions

In a nutshell, there is really not much new in the CIP-004-5 Requirements or Tables that we have not already been doing in Version 3. The same principles of Awareness, Training, PRAs and Revocation of Access are addressed, with just some changes in how the standard is formatted, for example, Tables instead of sub-requirements.
Questions?

Anyone? Bueller? Anyone?
Contact

Peter Scalici
Senior CIP Specialist
NPCC
1040 Avenue of the Americas
New York, New York 10018
E-Mail: pscalici@npcc.org (best way to contact)
Office: (212) 205-7065