Ask the Experts – Navigating Compliance Through the Coronavirus

Links and information from the webinar

View the webinar recording – https://archerint.com/events/navigating-compliance-through-the-coronavirus/

Official COVID-19 references mentioned during the webinar

March 10, 2020: High-level ESCC COVID Resource Guide:
https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Coronovirus_Resource_Guide_031020.ashx

March 18, 2020: FERC and NERC Statements
https://www.nerc.com/news/Headlines%20DL/FERC%20NERC%20031820%20final.pdf

March 23, 2020: ESCC Press Release
https://www.eei.org/resourcesandmedia/newsroom/Pages/Press%20Releases/3.23_ESCC_Covid-19_FINAL.pdf

March 30, 2020: Updated ESCC COVID Guide:
https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_COVID_Resource_Guide_v2-03242020.ashx?la=en&hash=D3732CBFB46827AA0331277E8D5CBE0CC4DFC3BF

March 31, 2020: List of activities NATF is taking:
https://www.natf.net/news/newsdetail/2020/03/31/coronavirus-planning-and-response

April 2, 2020: FERC Acts to Help Regulated Entities Manage Compliance
https://ferc.gov/media/news-releases/2020/2020-2/04-02-20-1.asp#.Xoz42y-z1uV

April 2, 2020: ESCC mission-essential workforce guide
https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Mission_Essential_Workforce_2020.ashx?la=en&hash=7618009ED20A06A987105A0817A180202406AFDF

April 6, 2020 - Motion to Defer Implementation of Seven Reliability Standards Due to COVID-19
https://www.nerc.com/news/Headlines%20DL/Motion%20to%20Defer%20Implementation%20of%20Reliability%20Standards.pdf

Follow-up Questions from the Webinar

Question: *What about TFEs?*
Answer: Operational infeasibility is an option, and filing a TFE may get you safe harbor until reviewed.

Question: *What are some of the creative approaches being taken by utilities to stay compliant?*
Answer: Some examples that were discussed within Archer after the webinar, are:

- During a CIP Exceptional Circumstance (CEC) you don't have to authorize electronic access. Personnel Risk Assessments (PRAs) are only required for authorized access. So, no PRAs during a CEC.
- If it is not possible to perform a full seven-year criminal history records check, conduct as much of the seven-year criminal history records check as possible and document the reason the full seven-year criminal history records check could not be performed. E.g. "not possible to perform due to time constraints."

Regional Resources for COVID-19

SERC: https://www.serc1.org/news/serc-news/2020/03/20/regulatory-discretion-during-covid-19-outbreak

MRO: https://www.mro.net/MRODocuments/Case-By-Case%20Noncompliance%20Notifications%20Related%20to%20Coronavirus.pdf

NPCC: https://www.npcc.org/Compliance/enforcement/Documents/NPCC%20COVID_19%20Exception%20to%20Compliance%20Tracking.pdf

Texas RE: https://www.texasre.org/CPDL/Texas%20RE%20Coronavirus%20Response%20Page.pdf

RF: https://rfirst.org/regulatory-discretion-for-covid-19-impacts

WECC:
https://www.wecc.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/CMEP%20instructions%20COVID-19.pdf&action=default

List of NERC CIP Standards where CIP Exceptional Circumstances (CEC) is allowed

CIP-004 R2, Part 2.2
Applicability: High-Impact BCS and their associated EACMS; and PCAs; Medium-Impact BCS with External Routable Connectivity and their associated EACMS and PCAs.
"Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances."

CIP-004 R4, Part 4.1
Applicability: High-Impact BCS and their associated EACMS; and PCAs; Medium-Impact BCS with External Routable Connectivity and their associated EACMS and PCAs.

"Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information."

CIP-006 R2, Part 2.1
Applicability: High-Impact BCS and their associated EACMS; and PCAs; Medium-Impact BCS with External Routable Connectivity and their associated EACMS and PCAs.

"Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances."

CIP-006 R2, Part 2.2
Applicability: High-Impact BCS and their associated EACMS; and PCAs; Medium-Impact BCS with External Routable Connectivity and their associated EACMS and PCAs

"Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances."

CIP-007 R4, Part 4.3
Applicability: High-Impact BCS and their associated EACMS, PACS and PCAs; Medium-Impact BCS at Control Centers and their associated EACMS, PACS and PCAs.

"Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances."

CIP-010 R3, Part 3.3
Applicability: High-Impact BCS and their associated EACMS and PCAs

"Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset."

CIP-010 R4
Applicability: High-impact and Medium Impact BCS and their associated PCAs

"Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1."