NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2016-02 Modifications to CIP Standards Drafting Team

February 16, 2023

Review NERC Antitrust Compliance Guidelines and Public Announcement

Jordan Mallory reviewed the NERC Antitrust Compliance Guidelines and noted that the meeting was public.

Roll Call

J. Mallory called roll. See page two.

Leadership Remarks

Matt Hyatt and Jay Cribb welcomed the drafting team and observers. M. Hyatt covered that the team would review an exclusion analysis created by Sharon Koller to assist the team on understanding the connections from CIP-010 to CIP-005 and CIP-007 based on Requirement R1 language. In addition, the team would take a look at proposals provided by some drafting team members and observers.

CIP-010 Modifications and Exclusion Analysis

S. Koller provided an overview of the *CIP-010 Requirement R1 Exclusion Analysis* she put together (See Attachment 2). She explained that Column C was the Draft 4 standards language; Column D was the technical control subject to CIP-010-5 R1 configuration change management; Column E was designed behaviors or expected outcomes of the system configuration; and Column F was for the team to consider if any exclusions were needed within CIP-010-5 based on discussion of each Requirement and sub-part.

Team members acknowledged how CIP-010 has been a hard standard to scope to virtualization changes and this spreadsheet provided good insight to help provide a better understanding for industry. It was discussed if the team should consider these sheets for the technical rationale document or maybe implementation guidance. An ERO Enterprise staff member spoke up that this document is very specific and would need some work and updating to help it meet the criterion for implantation guidance. The drafting team agreed that this document would provide good information, and would continue to think on the best place to house it as they continue modifications to CIP-010.

J. Cribb noted to the team that the teams draft three posting drafted subparts for the entity to identify impacted security controls in CIP-005 and CIP-007 and then to authorize those changes. He mentioned that the team would need to keep this in mind as modifications are being made to the CIP-010 standard as industry was not on board with the changes from draft three.

Scott Klauminzer provided proposed changes for the team's consideration as modifications to CIP-010 Requirement R1 and its subparts. High level list of those proposed changes:

- Update Requirement R1 language to state: "Authorize changes to Applicable Systems that alter one or more cyber security controls serving one or more Requirements in CIP-005 and CIP-007, as defined by the Responsible Entity."
- Remove "implementation" to avoid confusion
- Remove "may" as in "may alter" in order to more closely align with current CIP-010 R1 Part 1.1, for changes that alter the baseline, etc.
- Make cyber security controls flexible to "one or more"
- Align security controls with "one or more" Requires in CIP-005 & CIP-007, to reinforce that this is not about ALL requirements, just those being affected.

The drafting team agreed with these changes and updated the CIP-010 standard accordingly.

Future Meetings

a. March 9, 2023 | 1:00 – 3:00 p.m.

Adjourn

J. Mallory adjourned the meeting at 2:56 p.m. Eastern.

Attachment 1 Attendance				
Name	**Company**	**Member/ Observer**	**Straw Vote (X)**	**Conference Call/Web (Y/N)**
Jay Cribb	Southern Company	Co-Chair		Y
Matthew Hyatt	Georgia System Operations Corporation	Co-Chair		Y
Jake Brown	ERCOT	Member		Y
Norman Dang	Independent Electricity System Operator of Ontario	Member		Y
Robert Garcia	SPP, Inc.	Member		Y
Scott Klauminzer	Tacoma Public Utilities	Member		Y
Sharon Koller	ATC, LLC	Member		Y
Heather Morgan	EDP Renewables	Member		N
Mark Riley	Calpine	Member		N
Jordan Mallory	NERC	NERC Staff		Y
Marisa Hecht	NERC	NERC Staff		Y
Daniel Bogle	NERC	NERC Staff		N
Mike Keane	FERC	FERC Staff		Y
Jorge Reig	FERC	FERC Staff		N
Jenn Rinaldi	FERC	FERC Staff		Y
Ken Lanehome	Bonneville Power Administration	PMOS		N
Kirk Rosener	CPS Energy	PMOS		Y

Attachment 2

Standard	Req/Part	Draft 4 Proposed Language	Technical Control Subject to CIP-010-5 R1 Configuration Change Management	Designed Behavior(s) or Expected Outcomes of the System Configuration	Is a CIP-010-5 R1 Exclusion Needed?
CIP-005-8	R1	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-8 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	None. Process documentation is an administrative control	None	
CIP-005-8	R1.1	Applicable Systems connected to a network via a routable protocol must be protected by an ESP.	Changing the configuration that controls EAP to ESP or Changing the topology of the network connecting Applicable Systems is a change to technical control. (e.g. Dual homing a device inside the ESP by adding a network interface to a subnet outside the ESP)	Are there any automated actions taken in a Zero Trust configuration that could modify the EAP/ESP as a designed behavior?	
CIP-005-8	R1.2	Permit only needed routable protocol communications, and deny all other routable protocol communications, through the ESP; excluding time sensitive communications of Protection Systems.	Changing the configuration that controls the routable protocol communications through the ESP is a change to technical control.	Automated actions by the EAP to dynamically enable the routable protocol communications pathway on demand following sucessful authentication permitted through the EAP configuration is a designed behavior.	
CIP-005-8	R1.3	Permit only needed routable protocol communications to and from Management Interfaces of Applicable Systems, and deny all other routable protocol communications, per system capability.	Changing the configuration that controls the routable protocol communications that is permitted to Management Interfaces is a change to technical control.	Authorizing individuals for routable protocol communications to Management Interfaces is accomplished in CIP-004-8 R4, and excluded from CIP-010 R1. Changes to the list of authorized individuals and the Applicable System's automated actions to permit/deny that communcataions based on changes to the authorized list of individuals is a designed behavior.	
CIP-005-8	R1.4	Perform authentication when establishing Dial-up Connectivity with Applicable Systems, if any, and per system capability.	Changing the configuration that causes authentication to be required upon establishment of Dial-Up Connectivity is a change to a technical control.	Automated actions by the Applicable System to negotiate Dial-up Connectivity are a designed behavior (e.g. a Cisco router negotiating baud rate and adding it to the running configuration file)	
CIP-005-8	R1.5	Have one or more methods for detecting known or suspected malicious Internet Protocol (IP) communications entering or leaving an ESP.	Changing the configuration that controls how the detection method operates or what ESP ingress/egress communications it monitors is a change to a technical control.	Automated actions initiated by the deployed method and its configuration are a designed behavior (e.g. Intrusion Prevention System actions like dynamically shutting down communication pathways/ports on an EAP.)	
CIP-005-8	R1.6	Protect the data traversing communication links used to span a single ESP between PSPs through the use of: • Confidentiality and integrity controls, or • Physical controls that restrict access to the cabling and other non-programmable communication components in those instances when such cabling and components are located outside of a PSP, Excluding: i. Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012; and ii. Time-sensitive communication of Protection Systems.	Changing the configuration of electronic methods that controls how ESP-spanned data is protected in transit is a change to technical control. Changing the configuration of physical methods (if controlled by a PACS) that controls how cabling and other non-programmable communication components located outside of a PSP are protected when transmitting ESP-spanned data.	Automated establishment and teardown of protected communication paths is a designed behavior (e.g. A firewall or router dynamically enabling a VPN tunnel, assigning IP addresses/port/services for the session to communicate while established) Authorizing individuals for physical access to cabling and other non-programmable communication components located outside of a PSP is accomplished in CIP-004-8 R4, and excluded from CIP-010 R1. Changes to the list of individuals authorized for PSP access is a designed behavior.	
CIP-005-8	R2	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, per system capability, in CIP-005-8 Table R2 – Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	None. Process documentation is an administrative control	None	
CIP-005-8	R2.1	Permit authorized Interactive Remote Access (IRA), if any, only through an Intermediate System.	Changing the configuration that controls the path IRA may take as well as the specific interactive remote capability that is permitted to BCAs and their associated PCAs is a change to technical control.	Authorizing individuals for IRA through the Intermediate System is accomplished in CIP-004-8 R4, and excluded from CIP-010 R1. Changes to the list of individuals authorized for IRA and the Applicable System's automated actions to permit/deny IRA based on changes to the authorized list of individuals is a designed behavior.	
CIP-005-8	R2.2	Protect the confidentiality and integrity of IRA communications between the initiating Cyber Asset or Virtual Cyber Asset and the Intermediate System.	Changing the configuration of technical mechanisms that protect confidentiality and integrity of IRA communications is a change to a technical control.	Updating client side components to permit the use of technical mechanisms is a designed behavior (e.g. installing/updating a certificate, key, client software (ssh), enabling client side ports/services)	
CIP-005-8	R2.3	Require multi-factor authentication to the Intermediate System for all IRA.	Changing the configuration of or disabling settings that enforce the use of multi-factor authentication is a change to a technical control.	The automated action of the multi-factor solution changing the variable system-controlled authentication component (code, token etc.) or the manual action of the IRA user changing the user-controlled authentication component (pin, password etc.) is a designed behavior)	
CIP-005-8	R2.4	Have one or more methods for determining active vendor remote access sessions (including IRA and system-to system remote access).	If identity aware technology is implemented, changes to the configuration that controls the source which determines active vendor remote access sessions is a change to a technical control. Changing the configuration that controls which vendor systems can establish a remote access session is a change to a technical control.	Authorizing individuals to establish active vendor remote access sessions from vendor systems is accomplished in CIP-004-8 R4, and excluded from CIP-010 R1. Changes to the list of authorized individuals from vendors and the Applicable System's automated actions to permit/deny access based on changes to the authorized list of individuals is a designed behavior.	
CIP-005-8	R2.5	Have one or more method(s) to disable active vendor remote access (including IRA and system-to-system remote access).	Changing the configuration of the implemented method to disable active vendor remote access is a change to a technical control. (e.g. session idle timeout parameters, max session duration configuration, automated account/password expirations etc.)	Automated system action disable active vendor remote access is a designed behavior. If documented as one of the methods, manual actions to disable remote access could be argued are designed behavior (e.g. admin disconnects a session through shutting down a port, unplugging a cable, disabling a firewall rule, expiring a token, disabling a user or account etc.)	
CIP-005-8	R2.6	Intermediate Systems shall: 2.6.1. Not share CPU or memory resources with any part of a high or medium impact BCS; and 2.6.2. Restrict their routable protocol communications to BCS and their associated PCAs through an ESP.	Changing the configuration that controls separation of CPU or memory resources.	Automated actions by the system to dynamically 'move' tenants to assure separation of Intermediate Systems from any part of a high or medium impact BCS is maintained is a designed behavior.	
			Changing the configuration that controls the path routable protocol communications may take as well as the specific routable protocol communications that is permitted to BCAs and their associated PCAs is a change to technical control.	Automated actions by the system to permit/deny communications per the configuration is a designed behavior.	
CIP-005-8	R3	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-8 Table R3 –Vendor Remote Access Management for EACMS, PACS, and SCI. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	None. Process documentation is an administrative control	None	
CIP-005-8	R3.1	Have one or more method(s) to determine authenticated vendor initiated remote connections.	If identity aware technology is implemented, changes to the configuration that controls the source which determines authenticated vendor initiated remote connections is a change to a technical control. Changing the configuration that controls which vendor systems can initiate, authenticate, and establish a remote connection is a change to a technical control.	Authorizing individuals to initiate authenticate from vendor systems is accomplished in CIP-004-8 R4, and excluded from CIP-010 R1. Changes to the list of authorized individuals from vendors and the Applicable System's automated actions to permit/deny access based on changes to the authorized list of individuals is a designed behavior.	
CIP-005-8	R3.2	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	Changing the configuration of the implemented method to terminate authenticated vendor-initiated remote connections is a change to a technical control. (e.g. lock out a user/account, terminate session, block traffic from a specific source, etc.)	Automated system action to terminate authenticated vendor-initiated remote connections is a designed behavior.	
			Changing the configuration implemented method to control the ability to reconnect is also a change to a technical control. (e.g. a specific time interval to re-enable, a trigger following a quarantine action or other IPS function like blocking a port, service, IP source, or IP range.)	Automated action to permit reconnection after a predefined time interval, or after the system has determined threat has been addressed/mitigated could be argued is a designed behavior.	

Standard	Req/Part	Draft 4 Proposed Language	Technical Control Subject to CIP-010-5 R1 Configuration Change Management	Designed Behavior(s) or Expected Outcomes of the System Configuration	Is a CIP-010-5 R1 Exclusion Needed?
CIP-007-7	R1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-7 Table R1 – System Hardening. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]	None. Process documentation is an administrative control	None	No
CIP-007-7	R1.1	Disable or prevent unneeded routable protocol network accessibility on each Applicable System, per system capability.	Changing the configuration that controls what routable protocol network accessibility (which ports/services) are approved and permitted to be enabled is a change to a technical control.	Automated actions by the system to dynamically enable and use ports/services permitted through the configuration for protocol network accessibility is a designed behavior.	
CIP-007-7	R1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	Changing the configuration that controls what physical input/output ports are enabled for network connectivity, console commands, or Removable Media is a change to a technical control (e.g. The Network Access Control (NAC) configuration of a switch that specifies authorized MAC address). Changing the configuration that controls when/or under what confdltions devices are able to dynamically enable communication when connected to physical ports physical input/output ports is a change to a technical control.	Automated actions by the system to dynamically enable physical input/output ports permitted through the configuration is a designed behavior. (i.e. A TCA with a MAC Address matching the NAC configuration). Automated actions by the system to dynamically quaruntine and permit/deny access physical input/output ports based on security configuration is a designed behavior. (i.e. Malware Prevention tools auto-scans connected USB and permits mounting if drive is safe).	
CIP-007-7	R1.3	Mitigate the risk of CPU or memory vulnerabilities by preventing the sharing of CPU and memory resources, excluding storage resources, between Virtual Cyber Assets (VCAs) that are not of, or associated with, the same impact categorization.	Changing the configuration that controls separation of CPU or memory resources.	Automated actions by the system to dynamically 'move' tenants to assure separation is maintained.	
CIP-007-7	R2	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-7 Table R2 – Security Patch Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	None. Process documentation is an administrative control	None	No
CIP-007-7	R2.1	A patch management process for tracking, evaluating, and installing cyber security patches. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for Applicable Systems that are updateable and for which a patching source exists.	If using automated tools (i.e. Ivanti) to accomplish this for Applicable Systems that are updateable and for which a patching source exists, changing the configuration to exclude the tool from checking any such patch sources is a change to a technical control.	Automated actions by the system to dynamically evaluate and record the results of assessments for released patches from existing patch sources is a designed behavior.	
CIP-007-7	R2.2	At least once every 35 calendar days, evaluate cyber security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	If using automated tools (i.e. Ivanti) to accomplish this for Applicable Systems that are updateable and for which a patching source exists, changing the configuration of the cadence with which the tool performs an applicability evaluation change to a technical control.	Automated actions by the system to apply applicable patches is a designed behavior.	
CIP-007-7	R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each cyber security patch and a timeframe to complete these mitigations.	If using automated tools (i.e. Ivanti) to apply patches once determined applicable, changing the target Applicable systems, or disabling the automated pushes would be a change to a technical control.	Automated actions by the system apply the patches on a pre-approved cadence is an approved designed behavior.	
CIP-007-7	R2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	None. Mitigation documentation is an administrative control	None	No
CIP-007-7	R3	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-7 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].	None. Process documentation is an administrative control	None	No
CIP-007-7	R3.1	Deploy method(s) to deter, detect, or prevent malicious code.	Changing the configuration that controls how the deterrent, detection, or prevention method operates or what Applicable Systems it monitors, interrogates, or protects is a change to a technical control. (what and when to scan, or which hosts are whitelisted etc.) Installing/updating centralized server or client side software configured to deter, detect, or prevent malicious code is a change to a technical control.	Automated actions initiated by the deployed method and its configuration are a designed behavior (e.g. enabling a USB port to scan a connected USB.)	
CIP-007-7	R3.2	Mitigate the threat of detected malicious code.	Changing the configuration that controls the ability to detect malicious code so it may be mitigated is a change to a technical control. (uninstalling or disabling the reactive capability of the implemented method)	Automated actions initated by the configuration of the implemeted method are a designed behavior (e.g. eradicating, uninstalling, or quaruntining malware and wiping infected drive sectors, Intrusion Prevention System actions triggered by detected malicious code etc.)	
CIP-007-7	R3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Changing the system's processing configuration is a change to a technical control (e.g. signatures/patterns are auto-pushed to test each day at a specified time and a timed firewall rule automatically permits propogation to Applicable Systems at a 12 hour delay.) Changing the configuration of a centralized solution that controls the dissemination of patterns/siganture to clients is a change to a technical control. (e.g. chaging the IP address of a SIEM server) Changes to the client side/agent configuration that cause it to check for signature updates on a specific cadence.	Automated actions initiated by the implemented method and its configuration are a designed behavior (e.g. pushing or pulling pattern or signature updates)	
CIP-007-7	R4	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-7 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]	None. Process documentation is an administrative control	None	No
CIP-007-7	R4.1	Log security events, per system capability, for identification of, and after-the-fact investigations of, Cyber Security Incidents that include, at a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.	Changing the system's configuration that controls the type of events to log is a change to a technical control. (e.g. checkboxes enabling loggin of successful and failed attempts, settings that send detected malware events to a log) Changing the configuration of the log receiver that controls the transmission and injestion of logs such that collection will occur is a change to a techical control (e.g. chaging the IP address of a SIEM server)	None	No
CIP-007-7	R4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert that includes, as a minimum, each of the following types of events (per system capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Changing the configuration that specifies the types of events to detect, or the corresponding configuration to send the detected condition to an alerting engine (i.e. generate an alert) is a change to a technical control.	Automated actions initated by the configuration of the implemeted method are a designed behavior (e.g. eradicating, uninstalling, or quaruntining malware and wiping infected drive sectors, Intrusion Prevention System actions triggered by detected malicious code etc.) Automated actions by the system to enabel backup logging capabilities, if used. (e.g. dynamic enabling of alternate paths or methods to alert if the primarty method is down, like outbound opening/establishing a one-way outbound 'phone home' connection to send alerts.	
CIP-007-7	R4.3	Retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days, per system capability, except under CIP Exceptional Circumstances.	Changing the configuration that controls how long logs are saved	Automated actions to purge logs at less than 90 days due to system incapability is a designed behavior.	
CIP-007-7	R4.4	Review a summarization or sampling of logged security events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Changing the configuration that controls the summarization or sampling approach, the configuration of an automated preset interval, or the targets of the sample is a change to a technical control presumably set up to align with the Registered Entity's summarization or sampling detemination.	None	No
CIP-007-7	R5	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-7 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	None. Process documentation is an administrative control	None	No
CIP-007-7	R5.1	Have a method(s) to enforce authentication of interactive user access, per system capability.	Changing the configuration that controls the enforcement of authentication, or disabling enabled configuration parameters that permit enforcement capability to operate as configured is a change to a technical control.	The automated action of the multi-factor solution changing the variable system-controlled authentication component (code, token etc) or the manual action of the IRA user changing the user-controlled authentication component (pin, password etc.) is a designed behavior)	
CIP-007-7	R5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Changing the configuration or software composition that drive what default or generic accounts exist is a change to a technical control that invariably affects the ability to identify and inventory the specified account types. (Installing, updating, upgrading, or patching software)	None	No
CIP-007-7	R5.3	Identify individuals who have authorized access to shared accounts.	If identity aware technology is implemented, changes to the configuration that controls the source providing the identified authorized individuals is a change to a technical control.	Authorizing individuals for access to shared accounts is accomplished in CIP-004-8 R4, and excluded from CIP-010 R1. Automated actions to permit/deny access based on changes to the authorized list of individuals is a designed behavior.	
CIP-007-7	R5.4	Change known default passwords, per system capability	Changing the configuration to revert to default known passwords is a change to a technical control, whether it is a accomplished by re-enabling or reconfiguring disabled accounts, or by reverting config for enabled accounts to default through processes like system rebuild, application reinstallation, etc.	The user or automated system action of applying a secure password is a designed behavior.	
CIP-007-7	R5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Applicable Systems; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Applicable System.	Changing the configuration that control/enables the enforcement of password length and password complexity is a change to a technical control. Changing the specific configuration settings that determine the password length and the number/types of characters used for complexity is a change to a technical control.	The user or automated system action of applying a password that meets the length and complexity requirements is a is a designed behavior.	
CIP-007-7	R5.6	For password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months, per system capability.	Changing the configuration that expires passwords, disables accounts upon expiration, or provides warnings to users of pending expiration is a change to a technical control.	A user or automated system action of changing the password is a designed behavior.	
CIP-007-7	R5.7	Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts, per system capability.	Changing the configuration that sets the numeric limit to for the system to automatically act upon reached limits for unsuccessful authentication attempts is a change to a technical control. (e.g. lock out a user/account, terminate session, block traffic from a specific source, etc.)	Automated system action to prevent the unauthorized user from obtaining access once a configured limit is reached is a designed behavior.	
			Changing the configuration that controls when, or which conditions for the system to automatically revert the limiting action is also a change to a technical control. (e.g. a specific time interval to re-enable, a trigger following a quarantine action or other IPS function like blocking a port, service, IP source, or IP range.)	Automated action to reverse the automated response action after a predefined time interval, or after the system has determined threat has been addressed/mitigated could be argued is a designed behavior.	
			Changing the configuration that detects a configured threshold was met/exceeded, or the corresponding configuration to send the detected condition to an alerting engine (i.e. generate an alert) is a change to a technical control.	If in the documented process for R5, a manual response action to prevent the unauthorized user from obtaining access when an automated alert is received from threshold being met/exceeded could be argued is a designed behavior. If in the documented process for R5, manual action to reverse the response action after a predefined time interval, or after the Registered Entity has determined the threat has been addressed/mitigated could be argued is a designed behavior.	