1. General

1.1. Purpose

1.1.1. To manage and control the risk to the reliable operation of the Bulk Electric System (BES) located within the service territory footprint of Emera Maine (hereafter referred to as Emera Maine or the Company) from malicious or unintentional attacks on the BES Cyber Systems used to protect and operate the BES.

1.1.2. The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Emera Maine shall determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding responsibilities as defined in Emera Maine's relationships with other functional entities in the NERC Functional Model.

1.1.3. To detail the commitment and ability of Emera Maine management to incorporate and enforce the NERC Critical Infrastructure Protection (CIP) cyber security standards (CIP-002 to CIP-011).

1.2. Scope

1.2.1. This Policy establishes the principles to be used by Emera Maine for identifying, managing, and protecting *BES Cyber Systems* and their associated control and monitoring systems and information, owned or developed by Emera Maine.

1.2.2. This Policy applies to Emera Maine employees, including contract staff and temporary employees, as well as vendors, and other third parties who have authorized electronic or authorized unescorted physical access to *BES Cyber Systems* and to Emera Maine employees and vendor/service contractor personnel who do not have authorized access to *BES Cyber Systems* but are responsible for actions required to achieve and maintain compliance with NERC Reliability Standards CIP-002 through CIP-011.

1.2.3. The definition of terms used in this Policy appears in Attachment A.

1.2.4. Text contained with [ ] denotes the name of an electronic file documenting an internally developed process for the purpose of complying with a specific NERC CIP requirement or set of requirements.

1.3. Governing Principles

1.3.1. Emera Maine shall protect its BES Cyber Systems, such that, those assets continue to provide correct and reliable control, protection and operation of the Bulk Electric System during periods of normal operation and when subjected to directed intentional or unintentional cyber-attack.

1.3.2. Emera Maine shall protect its BES Cyber Systems when subjected to directed intentional cyber-attack, or other emergency situation(s), for which provisional actions are detailed in various Emera Maine Internal Reliability Processes.

1.3.3. This Policy shall be reviewed and authorized by the Emera Maine Senior Manager assigned with the overall responsibility for the implementation of and adherence to NERC Standards CIP-002 through CIP-011 at least every 15 calendar months and the Company shall retain documentation and records from the previous three calendar years to the present.

2. BES Cyber System Categorization

2.1. Methodology

2.1.1. To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

2.2. Categorization Criteria (CIP-002-5.1 R1)

2.2.1. The criteria defined in Attachment 1 of CIP Reliability Standard CIP-002-5.1 are used to categorize BES Cyber Systems into impact categories.

2.2.2. Requirement 1 of CIP-002-5.1 requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact. This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

2.3. Review & Approval (CIP-002-5.1 R2)

2.3.1. The list of Emera Maine impact criteria and associated control and monitoring devices developed through its categorization assessment shall be reviewed and approved by Emera Maine's CIPs Senior Manager at least every 15 calendar months and a signed record of such review.

3. Security Management Controls

3.1. Cyber Security Policy (CIP-003-6 R1 & R2)

3.1.1. Emera Maine shall document and implement a Cyber Security Policy [12.001] that represents Emera Maine's commitment and ability to secure its BES Cyber Systems.

3.1.2. Emera Maine shall ensure that its Cyber Security Policy is available to all personnel who have access to, or are responsible for, BES Cyber Systems. (http://www.emeramaine.com/media/1085/emeramainenerc-cip-cyber-security-policy.pdf)

3.1.3. Emera Maine's Cyber Security Policy shall be reviewed and approved at least every 15 months by the CIP Senior Manager assigned to lead and manage Emera Maine's implementation and adherence to NERC Reliability Standards CIP-002 through CIP-0011.

3.2. CIP Exceptional Circumstances (CIP-003-6 R1.1.9)

3.2.1. All CIP Exceptional Circumstances (per the definition) shall be reviewed, approved and documented per its internal reliability process [12.003] by the Senior Manager or an authorized delegate to ensure that the intent of this Policy is met.

3.2.2. CIP Exceptional Circumstances shall be reviewed and approved at least every 15 calendar months by the senior manager responsible for adherence to NERC Standards CIP-002 to CIP-011 to ensure that any and all past and present day exceptions are still required and valid.

3.2.3. Documented CIP Exceptional Circumstances must include an explanation as to why the exception is necessary and any compensating measures.

3.3. Senior Leadership (CIP-003-6 R3 & R4)

3.3.1. Emera Maine shall assign a senior manager with responsibility for leading and managing the entity's implementation and adherence of the NERC CIP-002 thru CIP-011 Standards per its internal reliability process [12.004].

3.3.2. Emera Maine shall ensure that the designated senior manager shall be identified by name, title and date of designation.

3.3.3. Emera Maine shall document changes to the designated senior manager within 30 calendar days of the effective date.

3.3.4. Emera Maine shall ensure that specific actions delegated by the senior manager to a named delegate or delegates shall be documented per its reliability process [12.004].

4. Personnel & Training

4.1. Security Awareness Program (CIP-004-6 R1)

4.1.1. Emera Maine shall establish, maintain and document its security awareness program [12.010] to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: direct communications; indirect communications; and management support.

4.2. Cyber Security Training Program (CIP-004-6 R2)

4.2.1. Emera Maine shall establish, maintain and document a cyber security training program [12.010] and shall ensure that all personnel having authorized access to BES Cyber Systems, including contractors and service vendors are trained prior to being granted access except in an emergency (as detailed in document [12.010]).

4.2.2. Emera Maine's training program [12.010] shall cover:

4.2.2.1. Cyber security policies;
4.2.2.2. Physical access controls;
4.2.2.3. Electronic access controls;
4.2.2.4. The visitor control program;
4.2.2.5. Handling of BES Cyber System Information and its storage;
4.2.2.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
4.2.2.7. Recovery plans for BES Cyber Systems;
4.2.2.8. Response to Cyber Security Incidents; and
4.2.2.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with removable media.

4.2.3. After initial training of personnel having granted authorized access to BES Cyber Systems, the Company shall ensure that follow-up training is provided every 15 months to persons with such access and that this activity shall be conducted and documented per its reliability process [12.010].

4.2.4. Emera Maine shall ensure that its cyber security training program [12.010] is

reviewed at least every 15 months and updated as necessary.

4.3. Personnel Risk Assessment Program (CIP-004-6 R3)

4.3.1. Emera Maine shall develop and document a personnel risk assessment program [12.010], in accordance with federal, state and local laws, and (subject to existing collective bargaining unit agreements), for personnel (including contractors or service vendors) having authorized cyber or authorized unescorted physical access to BES Cyber Systems.

4.3.2. Emera Maine shall ensure that its personnel risk assessment program [12.010] includes (at a minimum) the following:

4.3.2.1. That risk assessments are conducted prior to such personnel being granted authorized cyber or authorized unescorted physical access to BES Cyber Systems except in response to an emergency (see [12.003] for details),
4.3.2.2. Each assessment conducted shall include (at least) identity verification and a seven year criminal check, and
4.3.2.3. Each personnel risk assessment is updated at least every seven years after the initial personnel risk assessment or for cause.

4.3.3. The Personnel Risk Assessment Program must include a process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:

4.3.3.1. Current residence, regardless of duration; and
4.3.3.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more

4.3.4. Emera Maine shall ensure that the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to BES Cyber Systems is documented and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

4.4. Access Management Program (CIP-004-6 R4)

4.4.1. Process to authorize based on need, as determined by Emera Maine, except for

CIP Exceptional Circumstances:

4.4.1.1. Electronic access;

4.4.1.2. Unescorted physical access into a Physical Security Perimeter; and

4.4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

4.4.2. Emera Maine shall maintain lists of personnel with authorized cyber or authorized unescorted physical access to BES Cyber Systems, including their specific electronic (a.k.a. logical) and physical access rights to BES Cyber Systems following its internal reliability process [12.010].

4.4.3. Emera Maine shall ensure that maintained lists of personnel with authorized cyber or authorized unescorted physical access to BES Cyber Systems are reviewed quarterly and updated of any change of personnel with such access to BES Cyber Systems or any change in the access rights of such personnel. BHE shall ensure access list(s) with names of Emera Maine employees, contractors and service vendors are properly maintained.

4.4.4. For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that Emera Maine determines are necessary

4.4.5. Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that Emera Maine determines are necessary for performing assigned work functions.

4.5. Access Revocation (CIP-004-6 R5)

4.5.1. Emera Maine shall implement a process to initiate removal of an individual's ability for unescorted physical access and cyber access upon a termination action, and complete the removals within 24 hours of the termination action

4.5.2. For reassignments or transfers, Emera Maine shall revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that Emera Maine determines are not necessary by the end of the next calendar day following the date that Emera Maine determines that the individual no longer requires retention of that access.

4.5.3. For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic by the end of the next calendar day following the effective date of the termination action.

4.5.4. For termination actions, revoke the individual's non-shared user accounts within 30 calendar days of the effective date of the termination action.

4.5.5. For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action.

4.5.5.1. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that Emera Maine determines that the individual no longer require retention of that access.

4.5.5.2. If Emera Maine determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.

5. Electronic Security Perimeters

5.1. Electronic Security Perimeter (CIP-005-5 R1)

5.1.1. Emera Maine shall ensure that every Cyber Asset connected to a network via a routable protocol resides within an Electronic Security Perimeter [12.011] and that it shall identify and document the Electronic Security Perimeter(s) and all access points to these perimeter(s).

5.1.2. Emera Maine shall ensure all External Routable Connectivity must be through an identified Electronic Access Point (EAP).

5.1.3. Emera Maine shall require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

5.1.4. Where technically feasible, Emera Maine shall perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets, and

5.1.5. Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

5.2. Electronic Access Controls (CIP-005-5 R2)

5.2.1. If Emera Maine allows Interactive Remote Access to BES Cyber Systems Emera Maine shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible

5.2.1.1. Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

5.2.1.2. For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System

5.2.1.3. Require multi-factor authentication for all Interactive Remote Access sessions.

6. Physical Security of BES Cyber Systems

6.1. Physical Security Plan (CIP-006-6 R1)

6.1.1. Emera Maine shall document, maintain and implement a physical security plan [12.013] to restrict physical access to its BES Cyber Systems. This physical security plan must collectively include all of the following:

6.1.1.1. Definition of operational or procedural controls to restrict physical access.

6.1.1.2. Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.

6.1.1.3. Where technically feasible, utilize two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.

6.1.1.4. Means to monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

6.1.1.5. Process to issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

6.1.1.6. Means to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.

6.1.1.7. Process to issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection

6.1.1.8. Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.

6.1.1.9. Retention of physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days

6.2. **Visitor Control Program (CIP-006-6 R2)**

6.2.1. Emera Maine shall implement a visitor control program [12.013] for visitors (personnel without authorized unescorted access to a Physical Security Perimeter) that shall contain logs to document the date and time of entry and exit of visitors to and from Physical Security Perimeters (PSP) and that visitors within a PSP shall be continuously escorted by a person granted authorized unescorted access to the specific PSP.

6.3. **Maintenance & Testing Program (CIP-006-6 R3)**

6.3.1. Emera Maine shall implement a maintenance and testing program [12.014] to ensure that all physical security systems implemented to control, monitor and log physical access to BES Cyber Systems. At a minimum, the Company shall ensure that its maintenance and testing program includes:

6.3.1.1. Testing and maintenance of all physical security mechanisms at least every 24 months

6.3.1.2. Retention of testing and maintenance records

6.3.1.3. Retention of outage records regarding access controls, logging and monitoring for a minimum of one calendar year.

7. Systems Security Management

7.1. Ports & Services (CIP-007-6 R1)

7.1.1. Emera Maine shall establish, document and implement a process [12.016] to ensure that only those ports and services required for normal and emergency operations are enabled and shall disable other ports and services (including those used for testing purposes) prior to production including port ranges or services where needed to handle dynamic ports.

7.1.2. Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media

7.2. Security Patch Management (CIP-007-6 R2)

7.2.1. Emera Maine shall establish, document and implement a security patch management program [12.017] for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

7.2.2. At least once every 35 calendar days, Emera Maine shall evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 7.2.1.

7.2.3. For applicable patches identified in Part 7.2.2, within 35 calendar days of the evaluation completion, Emera Maine shall take one of the following actions:

7.2.3.1. Apply the applicable patches; or
7.2.3.2. Create a dated mitigation plan; or
7.2.3.3. Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

7.2.4. For each mitigation plan created or revised in Part 7.2.3, Emera Maine shall 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 7.2.3 is approved by the CIP Senior Manager or delegate

7.3. **Malicious Code Prevention (CIP-007-6 R3)**

7.3.1. Emera Maine shall deploy method(s) to deter, detect, or prevent malicious code. [12.018].

7.3.2. Emera Maine shall mitigate the threat of detected malicious code.

7.3.3. For those methods identified in Part 7.3.1 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.

7.4. **Security Event Monitoring (CIP-007-6 R4)**

7.4.1. Emera Maine shall log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:

7.4.1.1. Detected successful login attempts;
7.4.1.2. Detected failed access attempts and failed login attempts;
7.4.1.3. Detected malicious code.

7.4.2. Emera Maine shall 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 Cyber Asset or BES Cyber System capability):

7.4.2.1. Detected malicious code from Part 7.4.1; and
7.4.2.2. Detected failure of Part 7.4.1 event logging.

7.4.3. Where technically feasible, Emera Maine shall retain applicable event logs identified in Part 7.4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.

7.4.4. Emera Maine shall review a summarization or sampling of logged events as determined by Emera Maine at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

7.5. System Access Controls (CIP-007-6 R5)

7.5.1. Emera Maine shall have a method(s) to enforce authentication of interactive user access, where technically feasible. [12.019].

7.5.2. Emera Maine shall 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).

7.5.3. Emera Maine shall identify individuals who have authorized access to shared accounts.

7.5.4. Emera Maine shall change known default passwords, per Cyber Asset capability

7.5.5. For password-only authentication for interactive user access, either technically or procedurally Emera Maine shall enforce the following password parameters:

7.5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and

7.5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.

7.5.6. Where technically feasible, for password-only authentication for interactive user access, Emera Maine shall either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

7.5.7. Where technically feasible, Emera Maine shall either:

7.5.7.1. Limit the number of unsuccessful authentication attempts; or

7.5.7.2. Generate alerts after a threshold of unsuccessful authentication attempts.

8. Incident Reporting & Response Planning

8.1. Cyber Security Incident Response Plan Specifications (CIP-008-5 R1)

8.1.1. Emera Maine shall develop and maintain a Cyber Security Incident Response Plan [12.024] and implement the plan in response to Cyber Security Incidents. The Company's Cyber Security Incident Response Plan shall address, at a minimum:

- One or more processes to identify, classify, and respond to Cyber Security Incidents.
- One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.
  - Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.
- The roles and responsibilities of Cyber Security Incident response groups or individuals.
- Incident handling procedures for Cyber Security Incidents.

8.2. Cyber Security Incident Response Plan Implementation and Testing (CIP-008-5 R2)

8.2.1. Emera Maine shall test each Cyber Security Incident response plan(s) at least once every 15 calendar months:

8.2.1.1. By responding to an actual Reportable Cyber Security Incident;

8.2.1.2. With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or

8.2.1.3. With an operational exercise of a Reportable Cyber Security Incident.

8.2.2. Emera Maine shall use the Cyber Security Incident response plan(s) under Requirement 8.1.1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident.

8.2.2.1. Document deviations from the plan(s) taken during the response to the incident or exercise.

8.2.3. Retain records related to Reportable Cyber Security Incidents for three calendar years.

8.3. **Cyber Security Incident Response Plan Review, Update, and Communication CIP-008-5 R3)**

8.3.1. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, Emera Maine shall:

8.3.1.1. Document any lessons learned or document the absence of any lessons learned;
8.3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and
8.3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.

8.3.2. No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that Emera Maine determines would impact the ability to execute the plan, Emera Maine shall:

8.3.2.1. Update the Cyber Security Incident response plan(s); and
8.3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.

9. Recovery Plans for BES Cyber Systems

9.1. Recovery Plan Specifications (CIP-009-6 R1)

9.1.1. Emera Maine shall develop and document recovery plans for its BES Cyber Systems that collectively include:

9.1.1.1. Conditions for activation of the recovery plan(s).
9.1.1.2. Roles and responsibilities of responders.
9.1.1.3. One or more processes for the backup and storage of information required to recover BES Cyber System functionality.
9.1.1.4. One or more processes to verify the successful completion of the backup processes in Part 9.1.1.3 and to address any backup failures.
9.1.1.5. One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s).
9.1.1.5.1. Data preservation should not impede or restrict recovery.

9.2. Recovery Plan Implementation and Testing (CIP-009-6 R2)

9.2.1. Test each of the recovery plans referenced in 9.1.1 at least once every 15 calendar months:

9.2.1.1. By recovering from an actual incident;
9.2.1.2. With a paper drill or tabletop exercise; or
9.2.1.3. With an operational exercise.

9.2.2. Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations.

9.2.2.1. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test

9.2.3. Test each of the recovery plans referenced in 9.1.1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.

9.2.3.1. An actual recovery response may substitute for an operational exercise.

9.3. Recovery Plan Review, Update and Communication (CIP-009-6 R3)

9.3.1. No later than 90 calendar days after completion of a recovery plan test or actual recovery, Emera Maine shall:

9.3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;
9.3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and
9.3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.

9.3.2. No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that Emera Maine determines would impact the ability to execute the recovery plan, Emera Maine shall:

9.3.2.1. Update the recovery plan; and
9.3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.

10. Configuration Change Management and Vulnerability Assessments

10.1. Configuration Change Management (CIP-010-2 R1)

10.1.1. Emera Maine shall develop a baseline configuration, individually or by group, which shall include the following items:

10.1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
10.1.1.2. Any commercially available or open-source application software (including version) intentionally installed;
10.1.1.3. Any custom software installed;
10.1.1.4. Any logical network accessible ports; and
10.1.1.5. Any security patches applied.

10.1.2. Emera Maine shall authorize and document changes that deviate from the existing baseline configuration.

10.1.3. For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

10.1.4. For a change that deviates from the existing baseline configuration, Emera Maine shall:

10.1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;
10.1.4.2. Following the change, verify that required cyber security controls determined in 10.1.4.1 are not adversely affected; and
10.1.4.3. Document the results of the verification.

10.1.5. Where technically feasible, for each change that deviates from the existing baseline configuration, Emera Maine shall:

10.1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely

affected; and

10.1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

10.2. **Configuration Monitoring (CIP-010-2 R2)**

10.2.1. Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in 10.1.1).

10.2.1.1. Document and investigate detected unauthorized changes.

10.3. **Vulnerability Assessments (CIP-010-2 R3)**

10.3.1. At least once every 15 calendar months, Emera Maine shall conduct a paper or active vulnerability assessment.

10.3.2. Where technically feasible, at least once every 36 calendar months, Emera Maine shall:

10.3.2.1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and

10.3.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.

10.3.3. 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.

10.3.4. Document the results of the assessments conducted according to Parts 10.3.1, 10.3.2, and 10.3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action

plan and the execution status of any remediation or mitigation action items.

10.4. **Transient & Removable Media (CIP-010-2 R4)**

10.4.1. For its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, Emera Maine 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 of the Standard.

11. Information Protection

11.1. Information Protection (CIP-011-2 R1)

11.1.1. Emera Maine shall document and implement one or more documented information protection program(s) that collectively includes [12.005]

11.1.1.1. Method(s) to identify information that meets the definition of BES Cyber System Information.

11.1.1.2. Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

11.2. BES Cyber Asset Reuse & Disposal (CIP-011-2 R2)

11.2.1. Emera Maine shall establish and implement formal methods, processes, and procedures [12.021] for the disposal or redeployment of BES Cyber Systems within its Electronic Security Perimeter(s). It shall ensure that prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), Emera Maine shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.

11.2.2. Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, Emera Maine shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

Version History

Version	Action	Date
1	Original	June 29, 2011
2	Corrected document references Section I item 3.2 Added language Section IX item 1.1 further specifying Emera Maine actions regarding access to CCAs during emergencies. Added document 12.024 to Related Document List	July 9, 2011
3	Change 2.2 to define applicability of policy to Emera Maine and non-Emera Maine personnel. Define the term “annually” as meaning once each calendar year Clarification of commitment and ability of Emera Maine to protect BES Cyber Systems during emergency situations. Minor grammatical edits Classification level changed from Proprietary to Unrestricted Signatory page changes	December 30, 2011
4	Signatory page change, Gerry Chasse appointed as BHE new President & COO Incorporate Version 3 changes into policy as appropriate	February 23, 2010

	Change all references of BHEC to Emera Maine	
5	Change various references of Version 2 to Version 3 Added Visitor Control program to Physical Security Perimeter Plan (Section VI) per new requirement of CIP-006-3 Added Matt Allen to signatory page and corrected name of Company's President to full name	October 25, 2010
6	Changed all references from "Bangor Hydro" to "Emera Maine" Updated titles on Signatory Page	February 14, 2014
7	Updated hyperlink to CSP on emeramaine.com	April 1, 2014
8	OVERHAUL OF PROCESS • Updated to conform to V5 Standards • Streamlined numbering scheme • Updated signatory page	December 14, 2015
9	Updated to adhere to NERC CIP V6 Standards	February 24, 2016
10	Update to document references	August 25, 2016

Approvals - Signatures

PREPARED: _____

Date: 8/26/2016

Matt Allen

Compliance, Security & Environmental Supervisor

Emera Maine

APPROVED: _____

Date: 09/15/2016

Lois Smith

Sr. Director, IT & Support Operations (CIP Senior Manager)

Emera Maine

APPROVED: 10/28/2016

Date: _____

Tim Pease

Director, Legal & Regulatory Affairs (FERC Compliance Officer)

Emera Maine