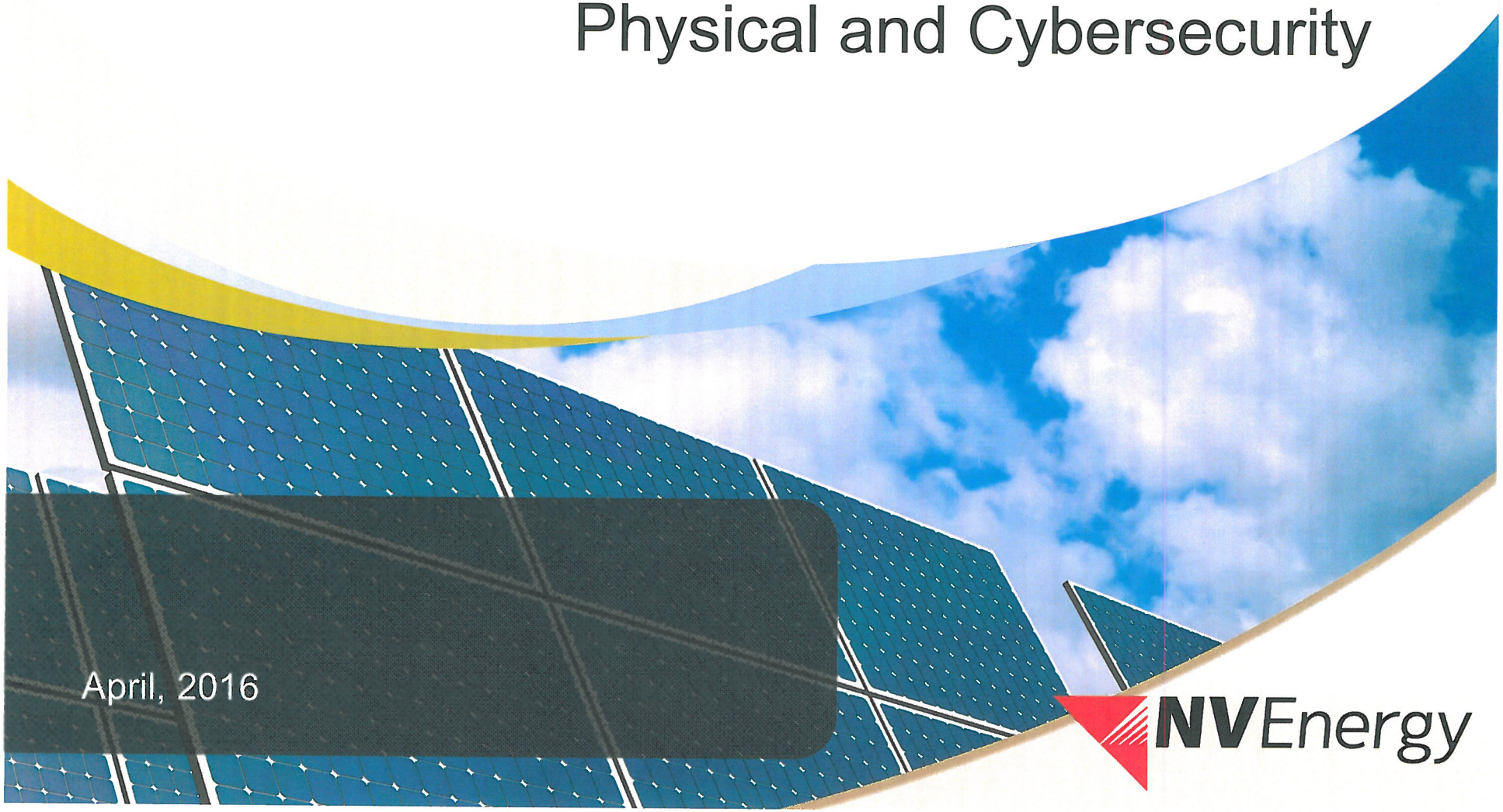
Grid Security

Physical and Cybersecurity



April, 2016

NVEnergy

Grid Security

- **Grid Security to protect the RELIABILITY of the Bulk Electric System (BES)**
  - Physical Security
  - Cybersecurity

- **Physical Security**
  - The purpose of physical security is to identify and protect transmission facilities and the associated control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection.

- **Cybersecurity**
  - The purpose of grid cybersecurity is to identify and protect critical cyber assets that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation or non-operation, adversely impact one or more grid facilities, systems, or equipment, which if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the power system.

NVEnergy

Grid Security

Background

- The Energy Policy Act of 2005 was signed into law August 8, 2005.
- Section 215 of the EPAct 2005 directed the Federal Energy Regulatory Commission (FERC) to certify an Electric Reliability Organization (ERO) and develop procedures for establishing, approving and enforcing electric reliability standards.
- The ERO selected was the North American Electric Reliability Corporation (NERC).
  - The Operations and Planning (O&P) Standards became mandatory and legally enforceable June 17, 2007 (FERC Order 693)
  - The Critical Infrastructure Protection (CIP) Standards became mandatory and legally enforceable December 2009 (FERC Order 706)

NVEnergy

Grid Security

The CIP Reliability Standards

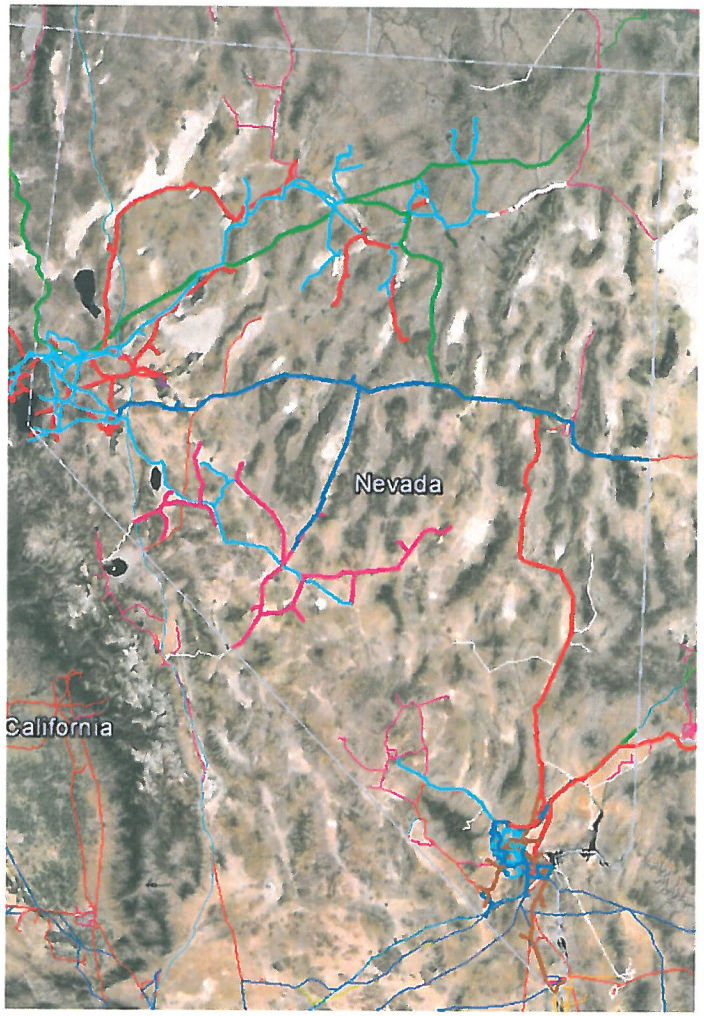
- **Physical Security** (CIP-014-2)
  - Physical Security of Cyber Assets (CIP-006-6)

- **Cybersecurity** (CIP-002, CIP-003, CIP-004, CIP-005, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011)
  - This family of Reliability Standards is often referred to as the CIPv5 Standards.

NVEnergy

Physical Security

- NV Energy performs risk assessments of our transmission substations (repeat every two-and-a-half years and includes planned facilities)
  - Including steady-state and transient analysis of the bulk electric system for loss of an entire facility accompanied by a bolted three-phase fault.
- Unaffiliated review by a third party (Utility System Efficiencies Inc. - 2015) to verify the risk assessment was adequate.
  - Review includes a verification of the NV Energy method to determine and prioritize each facility plus a technical review of the steady-state and transient analysis. NVE utilizes two 'independent reviews'.
- Facilities are categorized into four tiers based on risk to the reliability of the bulk electric system.



NVEnergy

Physical Security

- NV Energy then performs an evaluation of potential threats and vulnerabilities of a physical attack to the identified transmission facilities. The evaluation includes, but is not limited to;
  - any unique characteristics of the facility,
  - prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events, and
  - intelligence of threat warnings received from sources such as law enforcement, the North American Electric Reliability Corporation (NERC), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), and U.S. federal governmental agencies.

NVEnergy

Physical Security

- NV Energy develops and implements documented physical security plan(s) that cover the respective transmission facilities and associated control centers. The plans include, but are not limited to;
  - resiliency and security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential threats and vulnerabilities identified during the evaluation,
  - law enforcement contact and coordination information,
  - a timeline for executing the physical security enhancements and modifications specific in the physical security plan(s), and
  - provisions to evaluate evolving physical threats, and their corresponding security measures to the transmission facilities and the associated control centers.

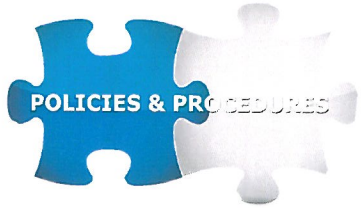
NVEnergy

Physical Security

- NV Energy utilizes an unaffiliated third party reviews of the evaluation performed and the security plan(s) developed.
  - Security Management International (SMI) (2016).
  - The Department of Homeland Security (DHS) (2016).
  - The security plan(s) are modified based on the review.

NVEnergy

Cybersecurity



- NV Energy developed, documented and implements a process to prioritize and categorize all facilities (and repeat annually).
  - There a four tiers based on risk impact to the bulk electric system.
- NV Energy implements a policy, company procedures and department plans to formalize NV Energy's critical infrastructure protection (review as needed but at least annually).
- Assigned an executive leader to direct and oversee the program.
- NV Energy implements an internal, but independent, review of the program annually including, but not limited to, a technical review of its application.

NVEnergy

Cybersecurity

- NV Energy developed, documented and implements a role based training program on an annual basis and for all new employees with either physical, electronic or information access to NV Energy bulk electric system cyber assets that can directly, or indirectly, affect the reliability of the bulk electric system.
  - This includes online training and face-to-face training.
  - The training includes a quiz and certification.
- NV Energy implements a quarterly awareness program including, but not limited to, signage, posters, emails, videos, departmental meetings, and talking points.

NVEnergy

Cybersecurity

- Physical, electronic and information access to cyber systems or associated information that can directly, or indirectly, affect the reliability of the bulk electric system is only granted on a need-to-know basis.
- NV Energy implements a personnel risk assessment program to those that require access, including but not limited to, a criminal history check, identification verification, and a seven year personnel risk assessment. Verification of the access lists and the appropriate personnel risk assessment results are performed quarterly. This applies to vendors and contractors as well.
- Physical, electronic and information access rights are reviewed on a quarterly basis.

NVEnergy

Cybersecurity

- All facilities identified in the top two tiers of the program are protected by an electronic security perimeter which includes, but is not limited to,
  - specific access points (e.g., firewall),
  - inbound/outbound access permissions including reason for access and denial by default,
  - intermediate remote access systems (DMZ),
  - encrypted networks, and
  - multi-factor and multi-layered authentication.

NVEnergy

Cybersecurity

- All cyber assets that can directly, or indirectly, effect the reliability of the bulk electric system receive, but are not limited to, the following security controls;
  - port and services protection,
  - security patch management,
    - including but not limited to, a monthly patch source tracking, evaluating, and application process
  - malicious code prevention,
    - including but not limited to, methods to deter, detect and prevent
  - security event monitoring, and
    - including but not limited to, alarming to electric system control center and physical security personnel.
  - access controls.
    - including but not limited to, complex password control and limited unsuccessful authentication attempts.

NVEnergy

Cybersecurity

- All facilities identified in the top two tiers of the program are protected by a hardened physical security perimeter which, includes, but is not limited to;
  - specific access points,
  - multi-factor authentication for access,
  - unauthorized access monitoring and alarming to NV Energy's electric system control center and physical security personnel,
  - physical access control device monitoring and alarming,
  - logging of all access,
  - continuous escorted access of all visitors, and
  - bi-annual maintenance of physical access control systems.
- Additionally, each facility has a site specific security plan including video surveillance.

NVEnergy

Cybersecurity

- NV Energy developed, documented and implements a cyber incident reporting and response plan. The plan includes, but is not limited to;
  - a process to identify and classify events,
  - a process to share incident reports with the appropriate authorities (DOE, ES-ISAC, etc.)
  - specific roles and responsibilities,
  - incident handling procedures,
  - annual exercise of the plan,
  - process to document deviations from the plan,
  - records of incidents, and
  - root cause analysis and lessons learned process for each event and deviation from the plan during events.

NVEnergy

Cybersecurity

- NV Energy developed and documented a cyber incident recovery plan. The plan includes, but is not limited to;
  - conditions to activate the plan,
  - roles and responsibilities,
  - process to backup and store data,
  - process to confirm successful back up of data,
  - process to preserve data,
  - annual exercise of the recovery plan,
  - annual check of preserved data, and
  - root cause analysis and lessons learned process for events.

NVEnergy

Cybersecurity

- NV Energy developed, documented and implements a change control process for all cyber assets that can directly, or indirectly, affect the reliability of the bulk electric system.
  - The change process includes monthly review of asset baselines.
  - Asset baselines include, but are not limited to, operating system/firmware, software, custom software, logical port identification, and security patches.
- Changes to baseline are required to go through a test sequence before being applied to the active environment.

NVEnergy

Cybersecurity

- NV Energy developed, documented and implemented a cyber vulnerability assessment program. The program includes, but is not limited to;
  - annual paper cyber vulnerability assessments of all tier one and tier two facilities,
  - triannual active cyber vulnerability assessments of all tier one and tier two facilities, and
  - reporting of all assessments including lessons learned and continuous improvement items.

NVEnergy

Cybersecurity

- NV Energy developed, documented and implemented a cyber information program for information that could directly, or indirectly, affect the reliability of the bulk electric system. The procedure(s) includes, but is not limited to;
  - a process to identify critical cyber information, and
  - a process to protect confidential cyber information.

NVEnergy

Cybersecurity

- All tier 3 and tier 4 facilities and the associated cyber assets include, at a minimum, a single form of physical access and electronic access control. Most facilities include a multi-layer access control system for both physical and electronic access.
  - NV Energy has plans to complete a more robust physical access control program for these facilities by 2018.

NVEnergy