Standard Name	Area	Description
CIP-001	Sabotage Reporting	This standard addresses Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.
CIP-002	Critical Cyber Assets	This standard addresses the identification and enumeration of Critical Cyber Assets. The standard calls for automating and routing the Critical Assets identification program throughout the network
CIP-003	Security Management Controls	This standard addresses the implementation of minimum security management controls in place as well as change management in order to protect Critical Cyber Assets.
CIP-004	Personnel and Training	
CIP-005	Electronic Security	This standard requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. It calls for provision a firewall in each access point, continuous monitoring and annual vulnerability assessment
CIP-006	Physical Security of Critical Cyber Assets	A physical security plan must be prepared so access control to critical assets is implemented and tracked. Unauthorized access must be immediately review and responded. Alarm mechXXsm must be installed and responded immediately
CIP-007	Systems Security Management	This standard requires that Responsible Entities have system security controls in force to detect, deter, and prevent the failure or compromise of critical functions performed by Critical Cyber Assets caused by mistake, misuse, or malicious activity.
CIP-008	Incident Reporting and Response Planning	This standard ensures the identification, classification, response and reporting of Cyber Security Incidents.
CIP-009	Recovery Plans for Critical Cyber Assets	This standard ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.
CIP-010	Configuration change management and vulnerability assessments	This standard ensures that unauthorized changes to Critical cyber assets are prevented and/or detected. In addition they also specifiy processes related to assessment of vulnerabilities in the system.
CIP-011	Information protection	This standard specifies requirements to protect information stored in the deployed system.

ORW Current Practice / Methodology
All ORW backend components such as AP, GW, EMS and OTV maintain extensive logs. This includes the ability to log all logon activity, configuration changes, device reloads/restarts, etc. The customer has the ability to save all these logs for the duration needed. These logs can then be used for periodic auditing purposes also. Note that CIP-001 will be retired in the future and moved to the Emergency Preparedness and Operations (EOP) set of standards.
The components of the ORW network do have unique identifiers; each node has a globally unique Node ID (NID), AP identified by MAC addresses, GW, EMS etc identified by the IPv4 addresses. Utility can mark these components as "critical" or "non-critical" based on their policies.
ORW backend network components support role based user accounts. ORW retains its own internal Change Management process for internal systems. ORW and the customer can jointly develop a Change Management process to exclusively address the deployed network and XX systems that may be collocated on the customer premises.
ORW network architecture recommends the use of stateful firewalls to create a ESP within which all Critical cyber assets reside. The node endpoints which lie outside the ESP are tightly controlled in terms of the traffic that they can send to the network. Firewall logs and data can be archived for security, review and compliance for a duration as determined by the customer.
The ORW backend network components provide for access control based on roles. Access can also be tied to Active Directory features. The endpoint security design ensures that only authorized devices can connect to and communicate with the network.
The ORW network provides information about unauthorized attempts to connect to and send data to the network. In addition, the ORW architecture allows for the seamless addition of various security focused entities such as IPS, IDS etc.
ORW components report security related events separately. These events include attempts to illegally access the network, attempts to pass unauthorized data in the network as also tamper detection attempts on end points and access points. Logs and data to be maintained for a duration as appropriate.
HA GW is addressed in a 2.x system. The KMS component needs to be in a secure facility and the data associated with KMS needs to be securely backed up. Other components of the ORW backend system are robust and recover from disasters.
The ORW system allows for changes to the system to be logged. The customer though has to ensure that they follow the standard practices to prevent unauthorized changes to the system. In addition, the ORW team constantly watches out for identified vulnerabilities in the deployed ORW software and takes preventive action when such software is identified.
The ORW system has been designed from ground up to provide secure communicaiton of information. This includes adherence to requirements associated with preventing leakage of information

CIP Standard Status (http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx)
Inactive
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Some portions here are subject to enforcement now and some subject to future enforcement
Subject to future enforcement
Subject to future enforcement