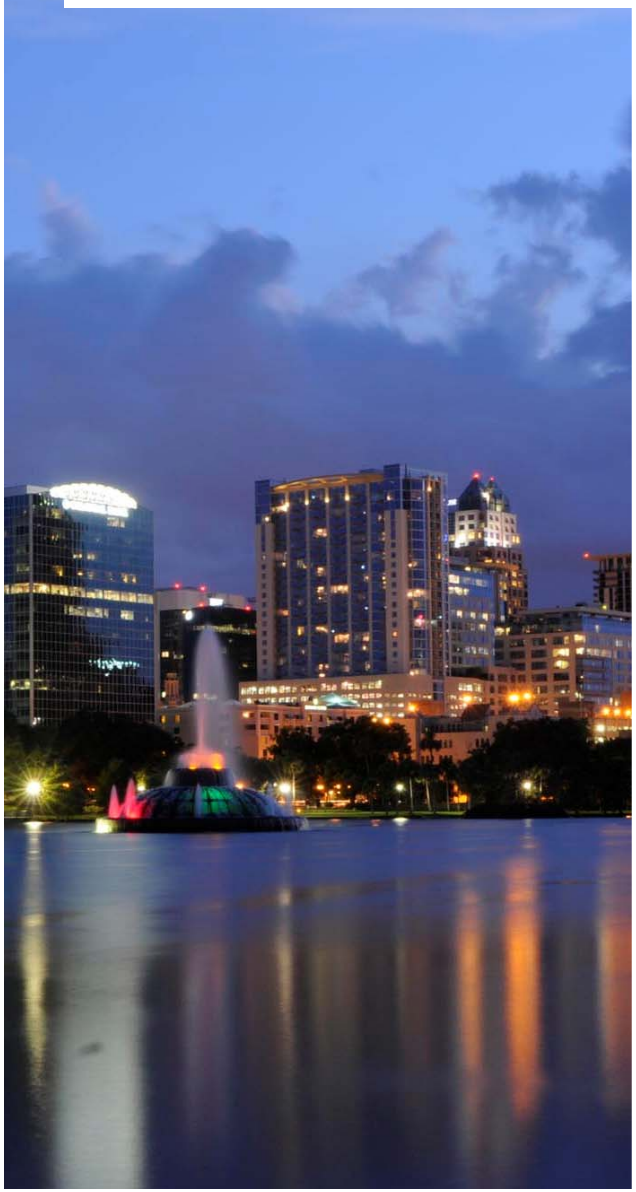


SIEMENS

How we support our customers with NERC CIP

James McQuiggan, CISSP

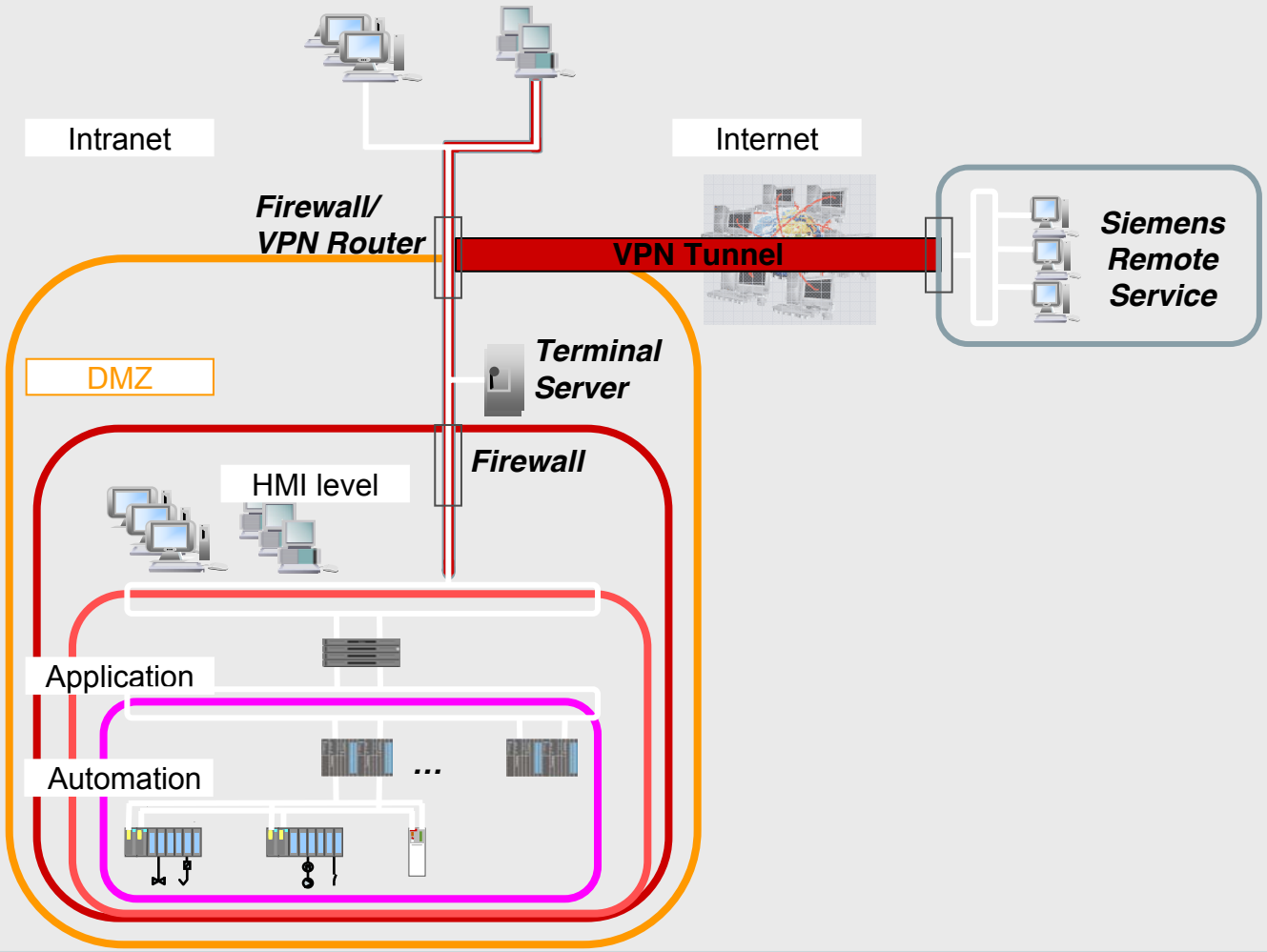
SIEMENS

Disclaimer

The information from this presentation is provided for informational purposes only. An customers adherence to the examples contained within this presentation does not constitute compliance with the NERC Compliance Monitoring and Enforcement Program ("CMEP") requirements, NERC Critical Infrastructure Protection ("CIP") Reliability Standards, or any other NERC Reliability Standards or rules. While the information included in this material may provide some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this material should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this presentation, to determine compliance with the CIP Reliability Standards.

SIEMENS

SPPA-T3000 Control System Security Features



- SPPA-T3000 ESP and security zone architecture (Defense in Depth)
- Secure remote access
- Monitoring
- Malware protection software
- Account management
- Security patch management

SIEMENS

NERC CIP Cyber Security Standards

CIP002-009 - Eight Standards / 41 Requirements

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009
CRITICAL CYBER ASSETS	**SECURITY MANAGEMENT CONTROLS**	**PERSONNEL AND TRAINING**	**ELECTRONIC SECURITY**	**PHYSICAL SECURITY**	**SYSTEMS SECURITY MANAGEMENT**	**INCIDENT REPORTING & RESPONSE PLANNING**	**RECOVERY PLANS FOR CCA**
1. CRITICAL ASSETS	1. CYBER SECURITY POLICY	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	1. PLAN	1. TEST PROCEDURES	1. CYBER SECURITY INCIDENT RESPONSE PLAN	1. RECOVERY PLANS
2. CRITICAL CYBER ASSETS	2. LEADERSHIP	2. TRAINING	2. ELECTRONIC ACCESS CONTROLS	2. PHYSICAL ACCESS CONTROLS	2. PORTS & SERVICES	2. DOCUMEN-TATION	2. EXERCISES
3. ANNUAL REVIEW	3. EXCEPTIONS	3. PERSONNEL RISK ASSESSMENT	3. MONITORING ELECTRONIC ACCESS	3. MONITORING PHYSICAL ACCESS	3. SECURITY PATCH MANAGEMENT		3. CHANGE CONTROL
4. ANNUAL APPROVAL	4. INFORMATION PROTECTION	4. ACCESS	4. CYBER VULNER-ABILITY ASSESSMENT	4. LOGGING PHYSICAL ACCESS	4. MALICIOUS SOFTWARE PREVENTION		4. BACKUP & RESTORE
	5. ACCESS CONTROL		5. DOCUMEN-TATION	5. ACCESS LOG RETENTION	5. ACCOUNT MANAGEMENT		5. TESTING BACKUP MEDIA
	6. CHANGE CONTROL			6. MAINTE-NANCE & TESTING	6. SECURITY STATUS MONITORING		
				Siemens Building Technology (SBT)	7. DISPOSAL OR REDEPLOY-MENT		
					8. CYBER VULNERABILITY ASSESSMENT		
					9. DOCUMEN-TATION		

BLACK – Customer Responsibility
RED – T3000 Feature
BLUE – Siemens Service

SIEMENS

CIP 003: Security Management Controls

SPPA-T3000 (Version 4.2) has been designed with the capability to meet applicable CIP 003 requirements

NERC Req.	NERC Comment	Siemens Solution
R1	Cyber Security Policy	
R2	Leadership	
R3	Exceptions	SPPA-T3000 Documentation
R4	Information Protection	Siemens Processes and Procedures
R5	Access Control	Siemens Processes and Procedures
R6	Change Control and Configuration Management	SPPA-T3000 Change Control and Configuration Management

SIEMENS

CIP 004: Personnel & Training

Siemens Approach to CIP 004 Requirements

NERC Req.	NERC Comment	Siemens Solution
R1	Awareness	Siemens Processes and Procedures
R2	Training	Siemens Processes and Procedures
R3	Personnel Risk Assessment	Siemens Processes and Procedures
R4	Access	Siemens Processes and Procedures

SIEMENS

Siemens NERC Policies

- Security Awareness Program
- Verifications
  - Secure web-based screening
  - ISO 9001:2000 certified
  - Local and state for all 50 states
- Siemens Critical Cyber Asset Training Program
- Customer Notifications – Notification within 24 hours of employee termination (policy in development)

- Bi-annual manager and employee online training
- New-hire orientation program
- Information security advisor program
- EnergyLine newsletter security articles/ reminders
- Internal control system – audits on information security

SIEMENS

NERC CIP Security Training

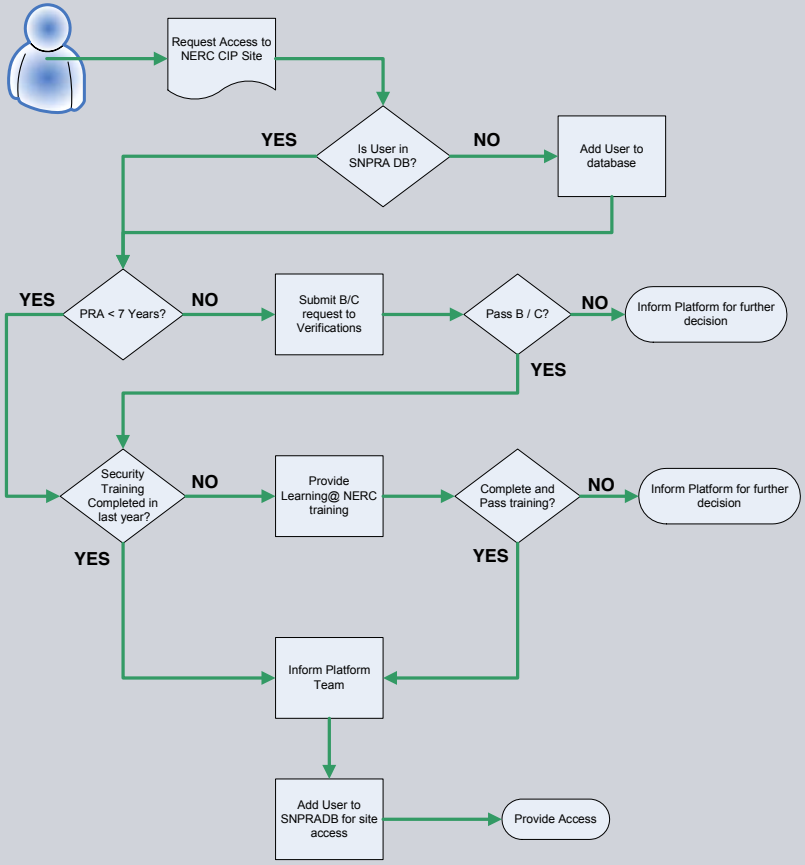
- Siemens Security Awareness Program
- For all Siemens employees with cyber or unescorted physical access to customer's Critical Cyber Assets
- Product training is provided for personnel utilizing T3000, TXP, or other Critical Cyber Assets at customer's plant
- Physical access might require additional customer training at site

Specific NERC CIP training program for CIP 004 Requirement 2

SIEMENS

Siemens Personal Risk Assessments (PRA)

- Establish a database to track the completed PRAs respective to customer sites.
- Process and procedures for:
  - Background checks
  - State / Federal / Criminal
  - Customer notification of changes to access lists:
    - Physical
    - Cyber



Siemens Policies & Procedures for CIP 004

SIEMENS

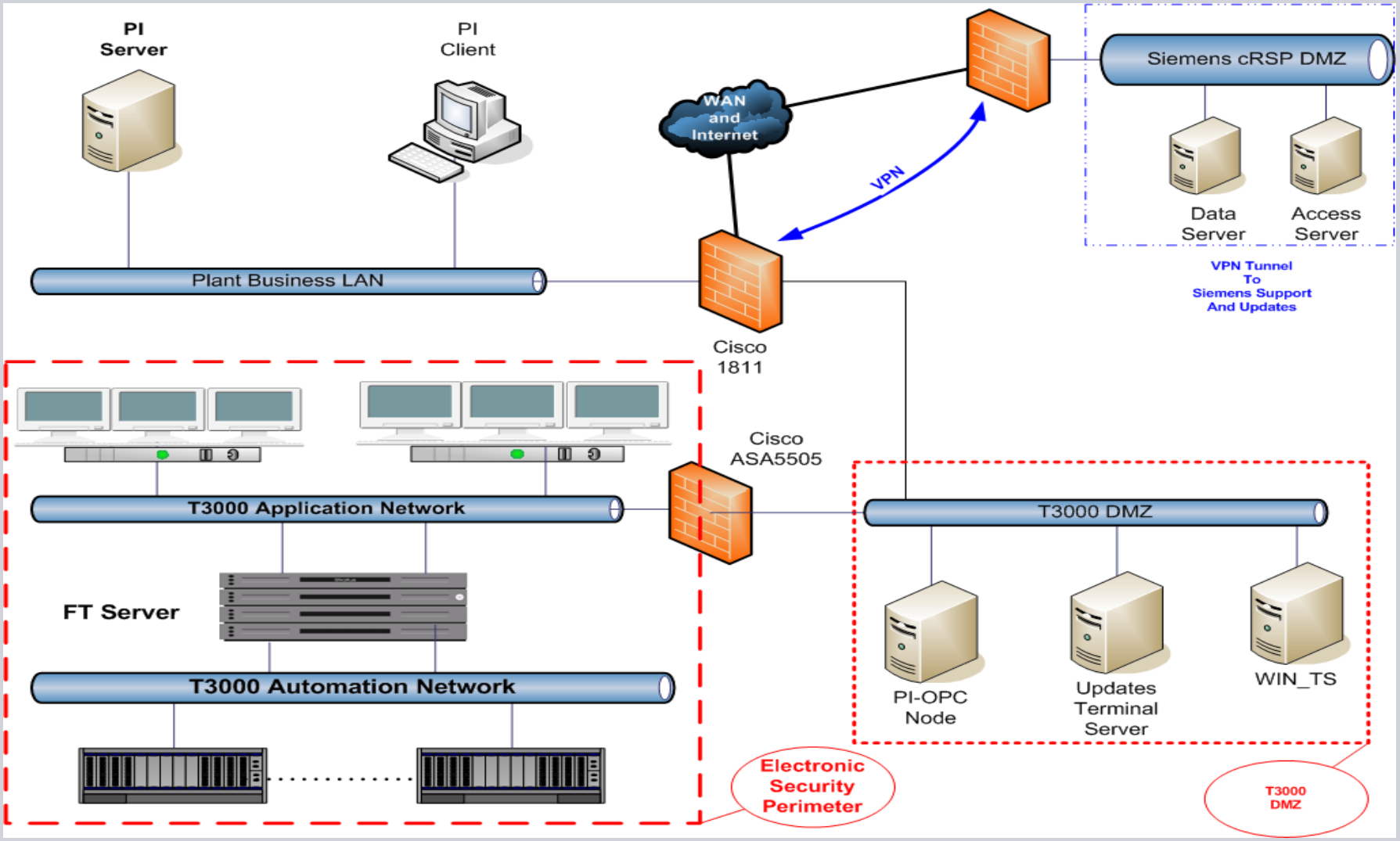
CIP 005: Electronic Security Perimeter

SPPA-T3000 (Version 4.2) has been designed with the capability to meet applicable CIP 005 requirements

NERC Req.	NERC Comment	Siemens Solution
R1	Electronic Security Perimeter	Security zone architecture of SPPA-T3000
R2	Electronic Access Controls	SPPA-T3000 Monitoring SPPA-T3000 Secure remote access
R3	Monitoring Electronic Access	SPPA-T3000 Monitoring
R4	Cyber Vulnerability Assessment	Siemens consulting services
R5	Documentation Review and Maintenance	SPPA-T3000 Documentation & Follow-up Long Term Support

SIEMENS

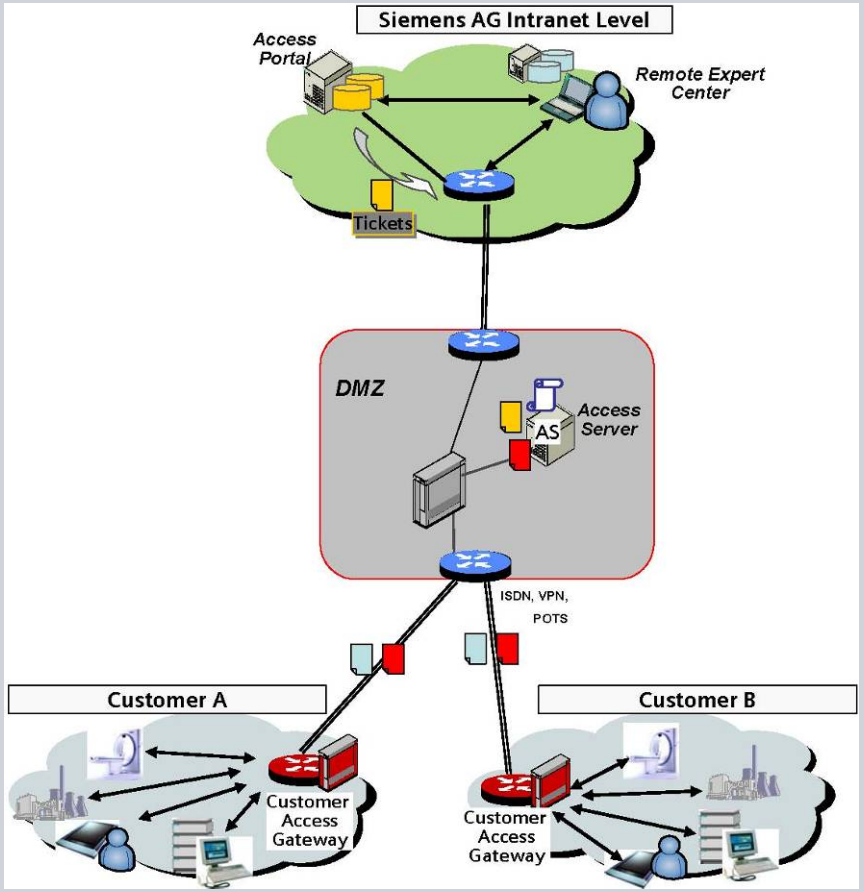
SPPA-T3000 Secure Network Architecture



SIEMENS

Siemens Remote Access (cRSP)

- common Remote Service Platform
  - Only on Siemens network
- Authorized users only
  - 2 Factor Authentication (PKI)
  - Grants
    - specific sites & application
  - Logging / Auditing
    - monthly reports / site
- Automatic Customer Notification



Siemens provides a remote solution for non-repudiation

SIEMENS

CIP 007: Systems Security Management

SPPA-T3000 (Version 4.2) CIP 007 Capabilities

NERC Req.	NERC Comment	Siemens Measures
R1	Test Procedures	ESP and Security zone architecture: SPPA-T3000 components are subject to security tests; non-SPPA-T3000 components are located outside of the ESP
R2	Ports and Services	SPPA-T3000 Hardening
R3	Security Patch Management	SPPA-T3000 Security patch management
R4	Malicious Software Prevention	SPPA-T3000 Malware protection software
R5	Account Management	SPPA-T3000 Monitoring and Account management
R6	Security Status Monitoring	SPPA-T3000 Monitoring
R7	Disposal or Redeployment	Siemens field service
R8	Cyber Vulnerability Assessment	Siemens consulting services
R9	Documentation Review and Maintenance	Siemens consulting services

SIEMENS

CIP 009: Recovery Plans for Critical Cyber Assets

SPPA-T3000 (Version 4.2) CIP 009 Capabilities

NERC Req.	NERC Comment	Siemens Measures
R1	Recovery Plans	SPPA-T3000 Emergency plan
R2	Exercises	Siemens training service
R3	Change Control	Siemens consulting service
R4	Backup and Restore	SPPA-T3000 Emergency plan
R5	Testing Backup Media	Siemens field service

Mapping the CIP Standards to Siemens competencies

SIEMENS

CIP Version 1 Current Standards

- CIP 001 – Sabotage Reporting
- CIP 002 – CCA Identification
- CIP 003 – Security Management
- CIP 004 – Personnel, Training
- CIP 005 – Electronic Security
- CIP 006 – Physical Security
- CIP 007 – Systems Security
- CIP 008 – Incident Reporting & Response
- CIP 009 – Recovery Plans

- Siemens CERT – Cyber asset security and expertise (003, 005,007)
- Global Data Pool – international personnel tracking and notification (004)
- Learn@ Siemens – NERC CIP CBT (004)
- Relationship with Verifications Inc (004)
- Information Security Program (004)
- Physical Security Expertise through Siemens Industry – Building Technologies Division (006)
- Expert I&C controls / Support (005, 007, 009)
- Member NERC Standards Committee (all)
- Security Consulting Services (all)
- CISSP, CPP Coordination (all)

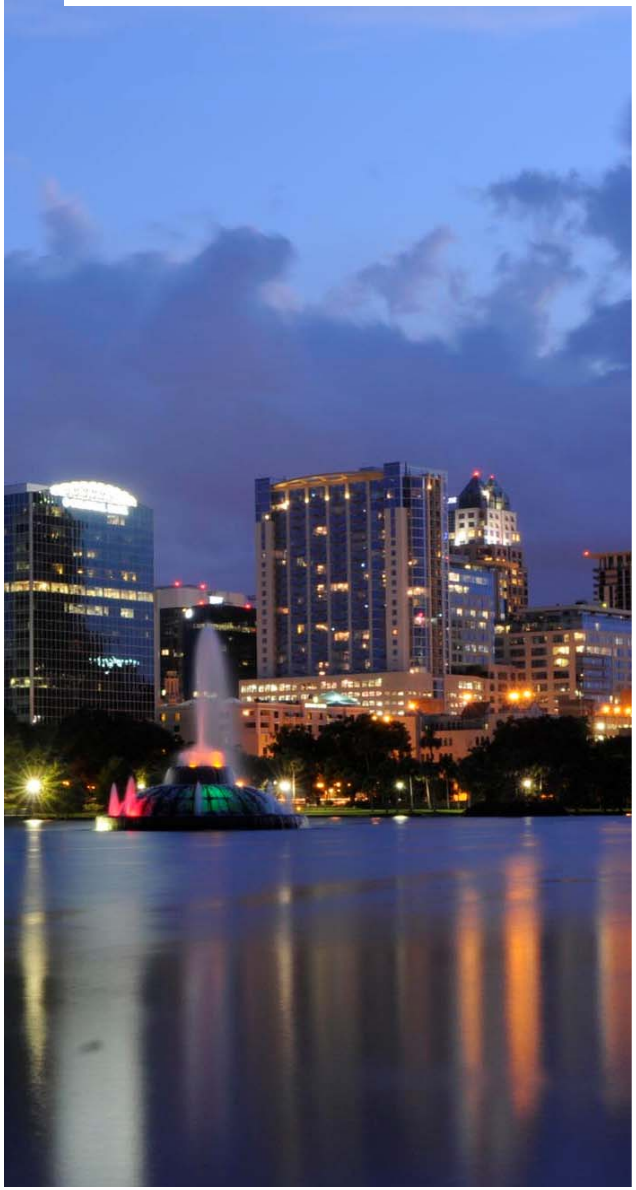
Siemens Capabilities to the NERC CIP Standards

SIEMENS

Siemens NERC CIP Contacts

- Siemens Customer – contact your Sales / Service Account Manager
- If you want to be a Siemens customer www.siemens.com/energy
- Siemens NERC CIP Questions:
  - James McQuiggan (james.mcquiggan@siemens.com)
  - Vladimir Vylkov (vladimir.vylkov@siemens.com)

SIEMENS



Thank you !